



Contract No.: DAMD17-99-C-9001

Defense Healthcare Information Assurance Program (DHIAP)

DHIAP Phase I Composite Evaluation Report

ATI IPS TR 00-02

February 2000

Prepared for:

U.S. Army Medical Research and Materiel Command

Fort Detrick

Frederick, Maryland 21702-5012

The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision unless so designated by other documentation.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 01-02-2000		2. REPORT TYPE		3. DATES COVERED (FROM - TO) xx-01-1999 to xx-06-1999	
4. TITLE AND SUBTITLE Defense Healthcare Information Assurance Program (DHIAP) Phase I Composite Evaluation Report Unclassified			5a. CONTRACT NUMBER DAMD17-99-C-9001		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Andrews, A. ; Packard, S. ; Alberts, C. ; White, T. ; Crane, L. ;			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME AND ADDRESS ATI 5300 International Blvd. N. Charleston, SC29418			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS USAMRAA 820 Chandler St. Ft. Detrick, MD21702-5014			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT APUBLIC RELEASE					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT See report.					
15. SUBJECT TERMS IATAC COLLECTION					
16. SECURITY CLASSIFICATION OF:		17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON	
		Public Release	84	email from Booz Allen Hamilton (IATAC), (blank) lfenster@dtic.mil	
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified		19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007	
				Standard Form 298 (Rev. 8-98) Prescribed by ANSI Std Z39.18	

REPORT DOCUMENTATION PAGE			<i>Form Approved</i> <i>OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE February 2000		3. REPORT TYPE AND DATES COVERED Composite Rpt. of Phase I Security Evals., Jan-June 1999
4. TITLE AND SUBTITLE Defense Healthcare Information Assurance Program (DHIAP) Phase I Composite Evaluation Report			5. FUNDING NUMBERS DAMD17 – 99 – C – 9001	
6. AUTHORS A. Andrews, ATI; S. Packard, LMES; C. Alberts, SEI; T. White, ADL; L. Crane, ATI, editor				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) ATI 5300 International Blvd. N. Charleston, SC 29418			8. PERFORMING ORGANIZATION REPORT NUMBER ATI IPS TR 00-02	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) USAMRAA 820 Chandler St. Ft. Detrick, MD 21702-5014			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS			12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words) This report provides a composite view of the findings and conclusions of the MTF Information Security Evaluations conducted as part of DHIAP Phase I. Research found that the security of patient information in the military medical system can be compromised and is at risk. Vulnerabilities are inherent at the local MTF level, caused in part by the centralized selection, administration, and maintenance of mandated health information systems. The report provides two perspectives on DHIAP Phase I research findings and recommendations. The first outlines, for nine technical and organizational investigation subjects, the vulnerabilities and risks that were identified and provides subject-specific recommendations for remedial action. The second, derived from the same material, provides information that crosses the boundaries of the investigation subjects to outline recommended activity according to such organizational focus areas as policy definition, procedure development, and training. Each of the assessments highlights the requirement for formulation of clear policy guidance, supported by assessment of the operational needs that drive the policy and the requirement to address personnel issues to implement and enforce the guidance. The cultural issues forced by addressing policy, operational, and personnel issues are supplemented and supported by improvements in technical tools and procedures.				
14. SUBJECT TERMS Information Security, Information Technology, Information Assurance, Computer Security, Healthcare Information Systems			15. NUMBER OF PAGES 73	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL	



DHIAP Phase I Composite Evaluation Report

ATI IPS TR 00-02

Authors:

Archie D. Andrews

Lynn S. Crane

Stephen L. Packard

Christopher Alberts

Thornton C. White

Contributors:

Robert A. Scudder Jr.

Jack A. Stinson Jr

Carla H. Decker

Forrest V. Schwengels II

Kevin J. Houle

Suresh Konda

James McCurley

Jeff Collmann

Willie Wright

February 2000

Acknowledgments

Phase I Information Security Evaluations and the follow-on analysis of vulnerabilities were conducted under the auspices of the Telemedicine and Advanced Technology Research Center (TATRC) of the Medical Research and Materiel Command (MRMC). The strength and validity of the research results is derived from the strength of the staff who participated: the DHIAP Team included experts in information protection, security, and healthcare, and each MTF site team was designed to include representatives of management and front-line staff from healthcare administration, clinical, and Information Management groups.

The DHIAP Team benefited significantly from input from two sources involved in Phase I research. First, the MTF site participants were both technically strong and eager to improve MTF ability to strengthen information assurance of patient and clinical information. The value of the information provided in this report is directly attributable to their willingness to share concerns, suggestions for improvement, and obvious confidence that it would be possible to successfully address the identified problems. Second, the TATRC participants were persistent in advising that people, their attitudes, and their work practices were part of the problem and had to be a significant part of the solution. This insight proved invaluable as the DHIAP “technology” investigation identified the necessity for integration of policy, operations, personnel, and technology focus areas to address vulnerabilities in protection of military information.

The authors acknowledge the document production and review contribution of Ms. Sarah Hartline of ATI. The quality of the document was greatly enhanced by her contributions.

TABLE OF CONTENTS

<i>Executive Summary</i>	<i>iii</i>
<i>I. Introduction</i>	<i>1</i>
Background	1
Purpose	2
Report Organization	2
Intended Audience	3
<i>II. Information Security Evaluation (ISE) Process</i>	<i>5</i>
Participants and Roles	5
Overview of the ISE Process	5
Major Activities of an MTF ISE Investigation	6
<i>III. Observations and Actionable Items</i>	<i>7</i>
Organizational Climate	9
Security of Patient Information	12
Security Policy and Procedure	15
Staffing Support Impact on Security Policy and Procedures	18
External Access to MTF Systems and Applications	21
Systems Administration	24
Systems Administration - Configuration	24
Systems Administration - System Services	26
Systems Administration - Network Operation and Services	28
Systems Administration - Passwords and User Accounts	29
Security Training	31
Disaster Recovery and System Backups	33
Physical Security	34
<i>IV. Recommendations and Conclusions</i>	<i>37</i>
Changes Affecting MTFs Today	39
Recommendations for Management Action	40
Information Protection Oversight	40
Policy	41
Technology Standards	42
Procedures	43
Training	44
Organizational Responsibility / Authority for Security	44
Technology	45
CONCLUSIONS	46

<i>V. Appendices</i>	49
Appendix A - DHIAP Phase I Methodology	51
Appendix B - Company Profiles and Staff Bios	63
Appendix C - References	69
Appendix D - Acronyms and Abbreviations	71

Executive Summary

In 1997 Congress recommended a program to develop and demonstrate effective ways to secure military healthcare information systems. In response to that recommendation, the Defense Healthcare Information Assurance Program (DHIAP) was developed. Its purpose is to identify weaknesses in current medical information systems and to develop and demonstrate prototype systems that provide reliable access to healthcare information while protecting that information from unauthorized access or alteration. The initial step in accomplishing DHIAP's goal is reported here. Known as the Information Security Evaluation (ISE), it consisted of evaluating existing military medical information systems and their operational environments at military Medical Treatment Facility (MTF) sites to determine vulnerabilities in information assurance capabilities and recommending operational procedures and policies to address those vulnerabilities. This report provides the findings and conclusions of the DHIAP ISE effort.

The following major activities were completed during DHIAP ISEs: investigating characteristics of military medical information systems and typical MTF operational environments, identifying information assurance vulnerabilities in operational environments by on-site evaluations, and recommending enhancements to military policy and operational procedures to address the reported vulnerabilities. Knowledge gained from the ISE effort was then used to define requirements and develop prototype technologies to address specific vulnerabilities.¹ Rollout and field-testing of the technology prototype are currently in process, and results of that effort will be provided in a subsequent DHIAP technical report.

Phase I vulnerability research found that the security of patient information in the military medical system can be compromised and is at risk. Vulnerabilities at the local MTF level are in part caused by the centralized selection, administration, and maintenance of mandated health information systems. While concerted effort on implementation of current Army regulatory guidance will mitigate some of the identified vulnerabilities, others that are beyond the site's capability and authority to address will require action on the part of higher echelons. Further, the Military will face additional exposure when assessed against the emerging standards for privacy of individually identifiable health information that will be required under the pending legislation and regulatory guidance of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

This report provides two perspectives on the DHIAP Phase I research findings and recommendations. The first outlines, for nine technical and organizational investigation subjects, the vulnerabilities and risks that were identified and subject-specific suggested action items. The second, derived from the same material, provides information that crosses the boundaries of the investigation subjects and outlines recommended activity according to such organizational focus areas as policy definition, procedure development, and training. Each set of recommendations highlights the requirement for formulation of clear policy guidance, supported by assessment of the operational needs that drive the

¹ Prioritization of vulnerabilities, site priorities, and consideration of need for access control, authentication, authorization, and audit of remote access capability resulted in building a prototype technology to comply with the Army directive for Remote Access Dial-In Users Standard (RADIUS).

policy and the requirement to address personnel issues to implement and enforce the guidance. The cultural issues forced by addressing policy, operational, and personnel issues are supplemented and supported by improvements in technical tools and procedures.

The two types of recommendations contained in the report are provided to encourage action both within MTFs and at higher levels of authority. For mitigating specific vulnerability areas, Section III outlines actions to be taken at each level of command involved in the work. Identified vulnerabilities from such broad subjects as “Security of Patient Information” to specific technical subjects such as “External Access to MTF Systems” and “Systems Administration” each include recommendations for corrective action by several levels of authority. Recommendations for actionable items are directed toward higher echelons outside the MTF, MTF management, and management of Information Technology and Security groups within the MTF. In contrast, the perspective taken in Section IV’s recommendations cut across the vulnerability areas to provide recommendations along lines of management focus areas. Section IV outlines the need for the following activities to occur in order to establish a strong information protection culture throughout military medicine:

- **Management oversight** of implemented information protection capabilities and the emergence of new vulnerabilities;
- Refinement and promulgation of **policy** to require an information protection culture;
- Use of **technology standards** to enable certain security measures and monitor their effectiveness;
- Refinement or development of clear **procedures** and **staff training** to assure that the people at every organizational level perform their work in approved ways and are equipped to make proper decisions in the course of their daily work;
- Establishment of appropriate **organizational responsibility** for the security function at the MTF level and in the higher echelons; and
- Selection and proper application of appropriate **technology** to serve the information protection mission.

DHIAP’s goal is to identify technology solutions for vulnerabilities in the Military’s ability to protect healthcare information. However, it is evident from the results of the Phase I investigations that a multi-faceted solution is necessary. Neither technology enhancements nor carefully planned changes to current policies and procedure can alone solve current problems. Rather, the observed state calls for an approach that encompasses policy, operations, personnel, and technology. Any plan to address identified information assurance issues should start with a vision of where information assurance fits into the command’s policy and priorities. A comprehensive Information Assurance Policy that addresses information security in relation to operational requirements is needed to direct and guide the military’s information protection activity. As policy is promulgated to the diverse organizations involved with military health information from the agencies that select and implement systems to the MTFs that treat patients, it should be used to provide a unifying influence for defining Operational, Personnel, and Technical changes that will ensure protection of military healthcare information.

I. Introduction

BACKGROUND

The United States Congress, the Secretary of the Army, and the Chief Information Officer of the U.S. Army Medical Command recognize that the current medical information systems are vulnerable to attacks on the integrity and confidentiality of their healthcare information. To address these issues, Congress recommended a program to develop and demonstrate effective ways to secure military healthcare information systems.

In their normal operation, healthcare information systems create, store, access, transfer, and exchange sensitive but unclassified information. The challenge is to handle the information in such a way as to protect the privacy, confidentiality, and integrity of the data while still providing efficient and effective access to authorized users when and where needed. To meet this challenge and identify the most effective ways to integrate proper policies, procedures, methods, and technologies into existing military or healthcare information systems requires the following:

- An understanding of present, near term, and future regulations and requirements for assuring the privacy of healthcare information;
- An understanding of the present state of the information security within the healthcare community;
- An analysis and documentation of functional requirements to provide requisite security while minimizing impact on required operational effectiveness; and
- A demonstration in the healthcare domain by installation and operation of a prototype to evaluate the effectiveness and operational impact of proposed security improvements.

The Defense Healthcare Information Assurance Program (DHIAP) was developed to meet the Congressional and Army goals. The purpose of DHIAP is to assess the present state of information security within the military healthcare system and to demonstrate prototype systems that provide reliable access to military healthcare information systems while protecting that information from unauthorized access or alteration.

The initial step in accomplishing DHIAP's goal involved evaluating existing military medical information systems and their operational environments at military Medical Treatment Facilities (MTFs) against expert knowledge of security practices that should be in place and current Army regulatory guidance. The goals of this activity were to determine vulnerabilities in information assurance capabilities and recommend operational procedures and policies to address those vulnerabilities.² This activity,

² See **Appendix C** for a list of Army regulations applied in this investigation. Note that the pending legislation and regulatory guidance of Health Insurance Portability and Accountability Act of 1996 (HIPAA), expected to be effective in early 2000 and requiring compliance about two years afterwards, will further affect requirements for privacy of individually identifiable health information.

DHIAP PHASE I COMPOSITE EVALUATION REPORT

DHIAP's Information Security Evaluation (ISE) effort, was performed during the period, January through June 1999.

This "Composite Evaluation Report" provides the results of the evaluation, specific actions to address reported vulnerabilities, and recommendations to management for improving information protection within the Army's medical organizations.

PURPOSE

This report was compiled to provide Command and various military organizations with an assessment of current-day operational realities that permit exposure of military and healthcare information and provide recommendations for action. Based on information gathered in Phase I ISEs, it establishes a roadmap for DHIAP follow-on work and identifies information assurance areas that will benefit from Command attention. In addition to identifying vulnerabilities that should be addressed at the MTF level where the research investigations were performed, the report also highlights problem areas that lie outside the authority of the MTFs and must therefore be addressed by external military organizations with system-wide authority.

It is important to note that specific results of each MTF Information Security Evaluation were provided to the site in an Evaluation Exit Briefing. As explained to the sites, the observations and recommendations point to both general areas and specific issues that the DHIAP Team noted during the course of the evaluation. While exceptions to the observed issues were seen in some cases, the noted problems were considered by the Team to be sufficiently pervasive or significant as to warrant mention in this report. Some of the vulnerabilities identified and reported here will be resolved through continuing efforts by the DHIAP team and MTF staff in subsequent phases of DHIAP.

REPORT ORGANIZATION

This report presents the process used to evaluate the sites and observations with associated recommendations derived from the evaluations.

Section II - Information Security Evaluation Process describes the process used to conduct the information-gathering Information Security Evaluations at the selected MTFs. The description covers activities from site selection through development of this Composite Evaluation Report and refers to Appendix A for more detailed coverage of certain process steps.

Section III - Observations and Actionable Items contains a summary of the DHIAP Team's observations of vulnerabilities and risks and recommended actions for nine specific technical/organizational subjects of investigation. For each subject, there is a brief definition, a performance goal, a recap of the Team's observations, and lists for different levels of Command/management of actions to take in addressing the reported issues.

Section IV - Recommendations and Conclusions focuses on recommendations for actions that cut across Section III's observation categories, defined in the context of general business management responsibilities (e.g., policy definition, procedure definition, oversight, etc.). The material in Section IV was developed to deal with the

potential system-wide impact on information security; its observations and recommendations are generic enough to apply to other MTFs not included in this study.

Appendix A provides additional detail about certain ISE process steps, as well as examples of some materials that were used by the DHIAP Team. Included as an attachment to Appendix A is a survey used with MTFs as a preliminary assessment of information assurance vulnerability.

Appendix B identifies and lists the credentials of the DHIAP Team members participating in the evaluations, both organizational and individual.

Appendix C lists reference documents used by the Team to increase their understanding of the existing and planned military operations, policies, and procedures.

Appendix D is a listing of the acronyms and abbreviations used in this report.

INTENDED AUDIENCE

This document is intended to serve as a report of risks and vulnerabilities found and recommendations for mitigating those findings. It became evident in the development of the report that there exist multiple audiences for this information.

- Because the observations and recommendations could be equally applicable to the daily operations of any MTF, other sites may be interested in this report as a resource for identifying and addressing immediate operational problems or concerns that may exist within their own environment.
- Additionally, as made clear by the evaluated sites during the presentation of findings, not all problems were in the scope of their authority or ability to address.

Thus, this report addresses an additional audience—those entities with broad regional or Command authority and responsibilities. It is the DHIAP Team's hope that the observations and recommendations provide sufficient clarity to support the Command actions required for resolving the identified issues.

II. Information Security Evaluation (ISE) Process

This section provides a synopsis of the Information Security Evaluation process as it was adapted and applied to the MTFs participating in the DHIAP.

PARTICIPANTS AND ROLES

The DHIAP ISEs were conducted under the auspices of the Telemedicine and Advanced Technology Research Center (TATRC) of the Medical Research and Materiel Command (MRMC). Members of the DHIAP Team of information protection, security, and healthcare experts included the following organizations.

- **ATI** (Advanced Technology Institute): Information Protection Solutions group
- **LMES** (Lockheed Martin Energy Systems): Data Systems Research Division
- **SEI** (Software Engineering Institute): CERT Coordination Center
- **HOST** (Healthcare Open Systems & Trials) consortium
- **ADL** (Arthur D. Little, Inc.): ISE Team coordination
- **Government representatives** from TATRC/MRMC

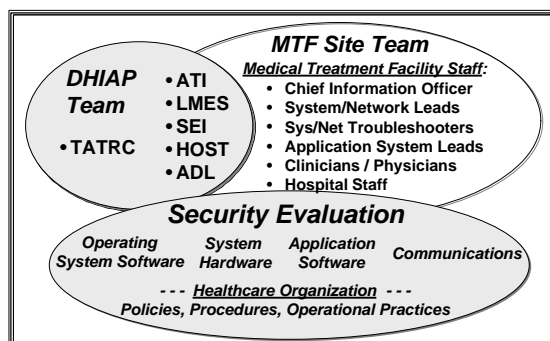


Figure 1 - DHIAP-ISE Team Members and Focus Areas

In addition, each MTF included in an ISE contributed the time of its Information Management staff, healthcare administrators, and clinicians. **Figure 1** above illustrates the organizations represented on the DHIAP Team, the types of team members contributed by the MTF, and the major subject areas addressed in the ISE process.

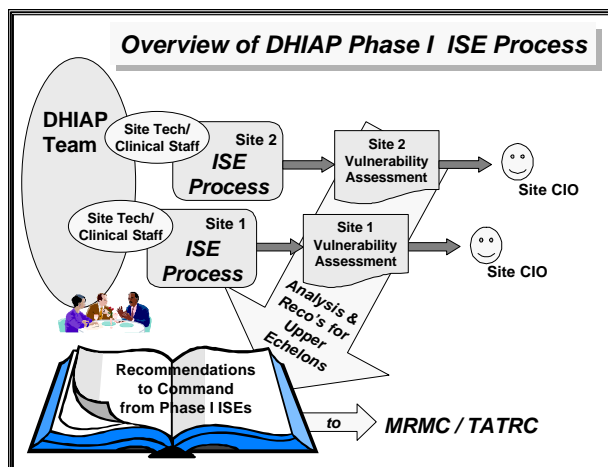


Figure 2 – DHIAP Information Security Evaluation Process

Phase I of the DHIAP, the Team worked with designated staff of each MTF being

OVERVIEW OF THE ISE PROCESS

The overall process planned for the DHIAP Team was to investigate security vulnerabilities at a representative set of military MTFs, as shown in **Figure 2**.³ After TATRC identified two MTFs for evaluation in

³ Original plans had called for two ISEs to be conducted at one of the sites, making a total of three ISEs, but it was later deemed unnecessary to conduct the third ISE during DHIAP Phase I.

DHIAP PHASE I COMPOSITE EVALUATION REPORT

investigated to perform the sites' ISEs. Each MTF ISE investigation (described under the next heading) concluded with several forms of feedback to the site, as follows.

- A Site Vulnerability Assessment briefing outlined the Team's observations and recommendations of instances where site information was found vulnerable to exposure. This briefing was limited to the MTF site and the DHIAP team; it was presented to MTF leadership, the Chief Information Officer (CIO), and selected staff of the Information Management group.
- Supporting details and recommendations for specific technical issues were provided to the MTF staff during the course of the evaluation.
- Subsequent to the briefing, a report outlining specific system and network administration technical details was provided to the CIO.

Following completion of the scheduled Phase I ISEs, the DHIAP team clustered the observations from each site in various ways to identify information threats and vulnerabilities common to all sites. The result of that effort is this report of observations and associated recommendations outlining the major vulnerabilities encountered and the DHIAP Team's recommendations for actions to address the vulnerabilities.

MAJOR ACTIVITIES OF AN MTF ISE INVESTIGATION

ISE activity at an MTF site began with site nomination and selection. TATRC nominated a number of representative sites, explained the incentive for the nominated sites to participate, and requested initial site information to screen the sites down to a representative sample. The request for information took the form of a Preliminary Survey requesting basic information about the nominated sites' staff, installed systems, existing policy, current training, and current practices. Based on survey responses, TATRC, with the DHIAP Team, selected two MTFs to be the sites initially evaluated in the ISE. At each facility, the ISE team followed the process and general timeline that is shown in **Figure 3** and described in greater detail in **Appendix A** to this report.

The DHIAP Team concluded the evaluation activities by analyzing the observations and recommendations developed during all of the ISEs and developing Phase I summary materials and plans for Phase II work. This Composite ISE Report documents the Phase I summary of the types of vulnerabilities currently evident in the military MTFs and DHIAP recommendations for MRMCM/Upper Echelon actions.

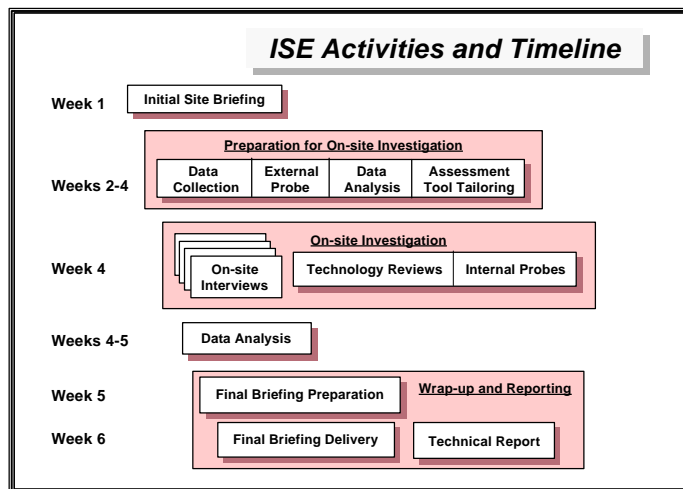


Figure 3 - Timeline and Activities of an MTF Vulnerability Assessment

III. Observations and Actionable Items

The observations and recommendations provided in this section were derived from specific findings of DHIAP Information Security Evaluations of a regional military MTF and its subordinate hospital MTF. The material is not site-specific and should not be construed as relating to a particular site. It is provided here because the identified vulnerabilities may be applicable to other sites and the recommendations address areas of concern at the organization and system levels. To restate a point made in Section II, all site-specific observations and recommendations were provided directly to each MTF upon completion of its evaluation, both as a formal presentation to the participants and also in the form of specific technical information detailing certain system configuration issues and recommended actions for mediation.

For many of the DHIAP Team's observations, the problem cannot be fully addressed at the local level. Higher-level action, by external Command and within the MTF, is required to establish commitment, provide resources, and/or assure the oversight needed for mediation of many reported vulnerabilities. This general DHIAP Team conclusion was confirmed in site feedback during the management briefing of observations/recommendations.

The degree of involvement and responsibility necessary among higher echelons and various MTF site roles in addressing the vulnerabilities reported in this document is depicted in **Figure 4**. The Observation/Actionable Item categories used in this section of

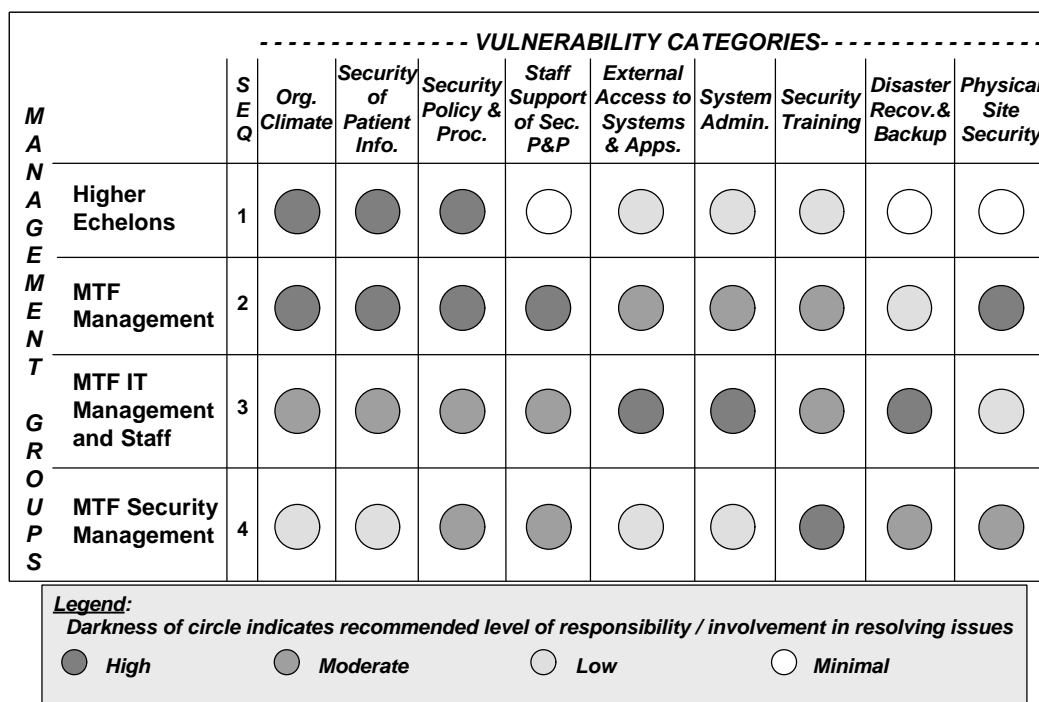


Figure 4 – Assessment of Management Group Level of Involvement in Addressing Vulnerabilities

the report are shown across the top of the diagram as “Vulnerabilities” (the definition of each of the categories will be found following the related heading in this section). Listed

on the left side of **Figure 4** are the management groups likely to participate in addressing the identified vulnerabilities. In very general terms, they refer to the following responsibility areas:

- Higher Echelons - External organizations at high levels of command; some are senior to the MTF in the line of authority, others are responsible for providing the computer systems and resources used at the MTF.
- MTF Management - Management personnel at MTF, in both clinical and administrative areas.
- MTF IT Management and Staff - Personnel within the information systems staff at the MTF; positions range from systems programmers to computer operators, programmers, and analysts.
- MTF Security Management - MTF staff responsible for managing the points of exposure such that normal processes are carried out in a secure manner.

[Note: the DHIAP team found that this Security Management group does not formally exist at this time. The duties and responsibilities were carried out with part-time support from various MTF departments. The establishment and delineation of responsibilities of this group is addressed in the Staffing Support Impact on Security Policy and Procedures section on page 18 and again with specific recommendations in section Organizational Responsibility / Authority for Security on page 44.]

In the body of **Figure 4**, the level of shading in each circle indicates the DHIAP Team's recommendation for level of responsibility and involvement of each Management Group in resolving issues of the Vulnerability Categories. This chart is included to suggest relative priorities of the various management groups. The gradation of the circles are based on a subjective judgement of the ability of the identified management group to effect change in the categories indicated. Security and all of its contributing components is everyone's responsibility but focusing management attention on those areas where they can have the most immediate impact should be useful.

As shown in **Figure 4**, higher echelon involvement or leadership is important to resolving vulnerability issues in many of the evaluation categories. It is also clear that protection of the information contained in MTF computer systems is not strictly a responsibility of the IT group at the MTF—although their ownership of certain mediation actions is essential. Involvement of the MTF Command is essential for implementing resolutions in every evaluation category. The reader will find that higher echelon activities focus on setting and implementing policy, providing policy guidance for development of procedures, and providing appropriate resources and processes to select, install, and maintain information systems for use within the MTFs. MTF Command activities will focus on confirming local policy, assuring strong guidance at the facility, and assuring that staff at the facility are made aware, properly trained, and motivated in information protection techniques and apply them in their daily work. The MTF's IT staff will carry responsibility for establishing and maintaining a technical environment that permits, enforces, and monitors compliance with information protection policy and procedure. Finally, Security Management will develop security policy for approval by the MTF Command, train staff at the facility in appropriate information protection techniques, use monitoring tools to

ensure compliance, reinforce appropriate action to encourage compliance with policy and procedures, and advise Command on security issues.

The remainder of Section III provides the DHIAP Team's specific Observations and associated suggestions for Actionable Items for the nine categories of investigation. (Note that the Systems Administration category is further divided into multiple technical areas.) The format followed in reporting each category, designed to provide the reader with both the context and specific focus within the area, is as follows:

- A description/definition providing a context for the remarks that follow;
- A Management Objective describing in general terms a performance standard for the area;
- Observations in the form of narrative descriptions of the potentially risky conditions, practices, and/or procedures observed by the Team during the course of the evaluation

(Note that, although exceptions to the Team's observations might be cited in some cases, the problems identified were considered sufficiently pervasive as to merit attention.); and

- Actionable Items grouped according to the type of staff who should be the focus of responsibility and authority

(Note that the Actions are specific to the context of the associated Observation. In some cases a specific action may be applicable to more than one observation area because of the high interdependence among the examined systems and the overlapping nature of the mediation actions that are needed. Actions that might be considered redundant were intentionally provided in each appropriate area so that each observation-action set could stand alone as a recommendation for action.).

ORGANIZATIONAL CLIMATE

We define organizational climate as the attitude that permeates an organization regarding a particular matter of Command and organizational interest. It is the ability of the organization to understand and interpret the intent of a policy because the guidance is ingrained throughout the organizational practices. The DHIAP Team based their observations in this area on interviews, both structured and one-on-one, with the staff from all areas of the MTF.

Management Objective:

Information Assurance policies and procedures are understood and endorsed throughout the organization. Members of the organization understand and support the policies and procedures well enough that they have no doubt how to react in situations not specifically covered by the existing guidance.

OBSERVATIONS:

The DHIAP Team observed a strong organizational concern for the security of sensitive healthcare information. They also observed a sense of frustration with current implementation of guidance that would address their concerns. The Team therefore concluded that information security was accorded low priority based on: the lack of clarity in information security guidance, their perception that MTF emphasis on information security was often more form than content, and their observations of apparent variations in application of security policies. This perceived lack of commitment to information security at MTFs was manifested by the frustration the staff felt in trying to enforce policy that was largely unwritten and therefore situation dependent. One member of the DHIAP Team observed that knowledge of security policy was being transferred as part of oral tradition.

The fact that the standards are unclear and unmeasured seemed to be the result of two attitudes prevailing within the sites' hierarchy. First, responsibility for implementing security in mandated systems belongs solely to the owners of the mandate (i.e., MEDCOM, etc.). Second, implementing sound security practices would conflict with "getting the job done."

The first attitude results in widespread reluctance to deal with the problems within the scope of their local authority, knowledge, skills and ability; it is not a shirking of responsibility so much as a ready acceptance of deferral of responsibility to higher echelons (USAMISSA, TIMPO, MEDCOM, etc.). The second attitude results in any conflict between mission and security resolving in favor of "the real job." The perception that MTF leadership believes security to be too costly or burdensome compared to benefits gained from enforcing it leads to exceptions becoming the norm. The two attitudes mentioned above appeared to be used for justifying shortcuts in lieu of addressing the issues where security is either impacted or perceived as a burden to operations.

Where individuals are aware of a security policy, they expressed a perception that the policy is applied unequally (e.g., observations that physicians have special status, are given special considerations in adhering to documented policies or mandated systems, and are not subject to the same security requirements as other staff). Staff frustration was fueled by having to deal with systems provided by outside organizations that varied significantly in their ability to consistently support the desired level of protection for sensitive information. It was also frustrating for support staff to deal with their perception that privileges and prerogatives associated with medical and military rank supplanted individual responsibility for security and reinforced a tolerance for the shortcut solution.

ACTIONABLE ITEMS:

Higher Echelons – Support for Security Policy and Procedures:

1. Establish information security as a Medical Command priority.
2. Provide defined policy for information security and related issues for Command and MTF activities.

3. Implement procedure to assist the MTF management, healthcare, and IT staff efforts to define more detailed policies and procedures for enforcing and monitoring compliance with security practices. Review policies and procedures developed to assure they fully support the Command's security initiative.
4. Institute a command-wide program for information security education/awareness to increase staff understanding of risks.
5. Assure that all levels of management plan to employ security practices appropriate to the risk.

Higher Echelons – Support for Computer Systems:

1. When selecting information systems provided by outside organizations, assure (via contract) that:
 - The delivered system will meet established security requirements (see recommendations for “External Access”) for user access, user identification and password, auditing, information security, etc.;
 - Implementation services will include adequate training and documentation for both user and systems support; and
 - Ongoing system support/maintenance provided by the outside organization will comply with established requirements for using secure communication methods and maintaining confidentiality of patient information.
2. Define standards that are to be followed by organizations outside the MTF (e.g., MEDCOM, TIMPO, USAMISSA, Tri-Care contractors, and third-party vendors). In addition to requiring compliance with Medical Command security policy, the standards should address the level and types of system implementation support that these organizations are required to provide to the MTF (e.g., resource planning for implementation and ongoing use of the system; analysis of operational impact of the system and the need for changing MTF security and operating procedures; resource planning for installation, use, and maintenance of hardware/software delivered with the system; etc.).
3. Provide the staff resources necessary to support implementation, ongoing use, and support of mandated systems installed at the MTF.

MTF Management:

1. Define operational standards with which new and existing systems must comply. Base these standards on higher echelon guidance, modified as required to incorporate local requirements.
2. Assure compliance with local operational standards by isolating any non-compliant systems from the other systems within the network.
3. Conduct internal campaigns to maintain MTF staff and employee awareness of the MTF Command's commitment to information security.

4. Assure that security procedures are applied equally at all levels and all types of MTF personnel. Deal with exceptions to security procedures by implementing an official forum for requesting, handling, and formally documenting resolution of the requests.

MTF Security Management:

1. Work with the operational organizations within the MTF to develop and enforce standard policy dealing with the details of operating interdependent systems in a secure manner.
2. Develop a campaign to ensure the policy is well understood and adhered to.

SECURITY OF PATIENT INFORMATION

The challenge in the MTF environment is to make the right data available at the right place and time to support the caregiver's information needs while protecting the patient's right to privacy and confidentiality. The Team based observations in this section on formal and informal interviews with MTF staff about the organization's ability to secure sensitive patient information.

MANAGEMENT OBJECTIVE:

Patient information is available only to authorized personnel at the time and place needed. Authorized access is based on user's identity, authorization, and need with regard to work to be performed at that time and at that location. Unauthorized access is precluded.

OBSERVATIONS:

MTF staff expressed concern about the lack of a definitive policy on patient privacy and confidentiality of patient information. They pointed out that patient information may be exposed in many ways, including: providing patient information telephonically to outsiders with minimal verification of the identity of the receiver/requestor; using non-secure e-mails to transmit patient information; accessing patient records from remote locations via public Internet; and leaving patient sign-in sheets in view of waiting patients and other visitors. It was pointed out in the interview process that there has been an increase in demand for access to patient information by non-MTF sources, and it was felt that responding to some of these requests for access increased the risk of unauthorized exposure of that information. Examples of external access to patient information include transferring patient information to managed care contractors and satisfying the increased requests for production of "ad hoc" reports.

The staff's concerns apparently stemmed from the mismatch between their perception of how patient records should be protected and their impressions of how the records are actually handled. There appeared to be three main areas of concern: access by external, and therefore suspect, agents; impact of technology on tracking and controlling access to sensitive information; and issues relating to patient permissions for how the information may be used.

Sensitive patient-identifiable information in electronic format was identified as at risk for exposure in a number of ways, including the following.

- Internal to the MTF, medical staff members maintain “convenience” files of patient information on their own or their departments’ computers. These unofficial personal databases are not subject to the IT Group’s official policies for information protection, purging, and quality checking.
- In normal day-to-day use of approved applications such as CHCS, the personal computers used as terminals hold patient information in cache memory as a normal byproduct of their use for system access.
- External providers of systems (i.e., the TriCare contractors and third party vendors who provide technical support for MTF systems/applications) have access to MTF patient data when they are providing system support.

The concern expressed by the staff illustrates a unique attribute of military medicine that needs to be considered: military staff members invest a significant amount of trust in the systems that support them. Military members and dependents, even though surrendering some personal prerogatives when they join the military, absorb the culture of trusting the military to protect the letter and the spirit of their implicit agreements. If that faith should be broken by such incidents as third party contractors marketing information on military members to outside agents, then a special trust will have been violated. Although not articulated, it appeared that MTF staff wholeheartedly accepted the responsibility of honoring the trust their clients vested in them and worried about their ability to fulfill the obligations of that trust.

Patient information recorded on paper is also exposed to risk; whether printed in authorized mode from MTF patient care computer systems or from the medical staff’s unofficial computer databases and systems, disposition of sensitive paper documents is weakly managed. Other types of paper records, such as ADS “Bubble Sheets,” are not covered well by management/disposition policies.

Apparently one of the reasons for the staff’s discomfort is a lack of understanding of the limitations and capabilities of the technology. It became clear that the pace of technology changes had outstripped policy guidance and the staff’s ability to assess the impact of change on their operations. The challenge with paper records had been to track them, provide physical security, and manage the flow of documents from record repository to care giver and back to the repository; the rules were clear and relatively easy to understand. With the advent of the hybrid record, part paper and part electronic, the rules have changed and the staff is less confident in understanding how to control proliferation of sensitive material. It becomes evident that the introduction of new technology must not only consider security of patient information but also address staff members’ comfort level with that security.

One other subject expressed as a concern in this area was confusion about the proper handling of the patient permission for how his/her medical information would be used. Medical staff expressed concern that patients understood neither the permission documents they were asked to sign nor what they were allowing to occur when granting blanket permissions. Concern was also expressed about the coverage of those permissions (e.g., whether third party vendors were subject to the same set of permissions and related restrictions as the MTF). The Staff Members felt they have an obligation to the patient to ensure that patients understand the meaning and ramifications of the permissions they are

asked to grant. However, they felt unable to satisfy this obligation because the policy defining the rights accorded to the military member who agreed to permission statements was unclear.

ACTIONABLE ITEMS:

Higher Echelons – Support for Security Policy and Procedures:

1. Clarify rights accorded to military members and their dependents regarding privacy of patient information. Where patient permission statements are used, assure they adequately describe how the information will be used.
2. Provide guidance and an appropriate standardized approach for sanitizing cache memory following downloading of sensitive information.

MTF Management:

1. Define and make widely available a comprehensive MTF policy for protecting patient privacy and the confidentiality of patient information to include requirements for patient permissions.
2. Assure that all MTF staff receive training appropriate to their position on policy and procedures for protection of patient information.

IT Group Management:

1. Develop a vulnerability profile outlining MTF-approved and unapproved methods by which patient information is shared with outsiders (e.g., telephone, fax) or might be exposed to outsiders/unauthorized MTF staff (e.g., open display of clinic patient sign-in sheets, unattended terminals involved in active sessions, etc.).
2. Define detailed policies and procedures to specifically address all situations noted in the vulnerability profile. Some known subjects to be covered by detailed procedure include the following:
 - Verifying the identity and security profiles of individuals who request new/modified access to systems and who request ad-hoc reports that include patient-identifiable information (including individuals who represent the external providers/maintainers of MTF systems, e.g., staff of MEDCOM-TIMPO-USAMISSA, Tri-Care contractors, and third-party vendors);
 - Assuring that third party payers are given only the information they are authorized to receive based on their contracts with the patient and the MTF;
 - Include terms and conditions in contracts with external agencies to ensure that protected health information disclosed to external agents remains confidential.
 - Verifying the identity of outsiders who request and/or are given patient information via telephone;
 - Tracking receipt and disposition of information faxed and/or mailed to outsiders to assure proper procedure is followed;
 - Securing e-mail transmission of patient information outside the Command;

- Including in the facility's portfolio of supported systems those MTF staff "convenience files" that are deemed necessary to providing quality care and make them subject to the same access and information protection procedures (e.g., audit compliance, backup/recovery, purging, etc.) as the "official" MTF systems;
 - Assuring that personal computers allowed to access patient information (e.g., CHCS terminals) do not retain the patient information in their cache memory when the session has ended;
 - Tracking use and disposition of paper copies of sensitive patient information (e.g., system-generated reports, forms completed by/for the patients, ADS bubble sheets, patient sign-in sheets); and
 - Tracking existence of non-standard software installed on MTF systems, determining whether they should be allowed, and assuring they do not have an adverse impact on overall processing of MTF systems.
3. Review and reinforce procedure and practice for obtaining, retaining, and using patients' permission/authorization for release of information from their files.
 4. Publish the new policy and procedures for assuring physical security of the MTF patient information and train staff in its use. To reduce the perception that rules are administered differently depending on staff role or other differentiator, assure that enforcement of the new procedures is evident to all staff members.
 5. Provide training and familiarization on new technology in the form of fact sheets for staff.

SECURITY POLICY AND PROCEDURE

Security policy and procedures are the tools an organization uses to implement information security practices. The policies provide the operational guidance for protecting sensitive information and form the basis for commonly accepted practice within an organization. The procedures address particular actions required and must be adapted to the operational needs and realities of the target organization. The DHIAP Team reached the following conclusions after examining published documentation that defines acceptable practices at the site and interviewing members of the staff and users about their understanding and implementation of practices.

MANAGEMENT OBJECTIVE:

Policies and procedures dealing with information assurance are sufficiently comprehensive that necessary exceptions are minimal. Personnel impacted by the policy are familiar with and follow its guidance. Procedures are applicable to the systems and operations addressed and are updated periodically to conform to changes in the technical, operational, and regulatory environment.

OBSERVATIONS:

In general, the DHIAP Team observed a disconnect between the policy and its implementation and varying degrees of frustration with policy implementation and enforcement. MTF policies often rely on individual interpretation and real-time, verbal guidance. This appeared to be the result of fragmented, incompletely documented, and inconsistently administered information security policy.

The technology implemented in the MTF IT environment is changing so rapidly that policy and user training are not keeping pace. Also, the degree of variance in the mandated systems' approaches to security affects the ability to create universally applicable policy guidance.

Operational necessities were often used as a rationale to bend security policy. Because operational considerations are used as justification for bending policy, exceptions to policy enforcement make the policy itself appear inconsistent. It appeared that the policies were being redefined based on situational conditions and there was frustration over defining acceptable and unacceptable behavior.

There appear to be many causes for the observed incongruities between policy and procedures including: dependence on multiple contractors and subcontractors; variable, system dependent training in security practices; delegation of responsibility for enforcement to the lowest possible level; and perception of a conflict between operational needs and sound security. The missing element appears to be an institutionalized process regarding information protection that consists of uniform security policies, procedures, and practices.

Policies for the following areas are in need of clear definition and implementation as operational procedures.

- Systems: Users and system administrators must often adjust MTF operations to fit with the characteristics of a particular system and/or develop unique approaches to security as a result of situations unique to the various installed systems.
- User Environment: Users who are unaware of the impact of security policies on operations increase the risks associated with sensitive information. As they retrieve information to their local system for operational convenience or fail to log off workstations, they compromise system/network access controls. Instances of unattended "active" terminals, use of access "work-arounds," and use of broad, role-based access authority all contribute to allowing the user community inappropriate access to patient information.

- User Convenience Practices: “Convenience” practices of some system users (e.g., clinical staff maintenance of unofficial hardcopy and electronic patient data in files that are outside of system control) jeopardize information security. It is common for some individuals to download patient information to local storage on unsecured systems, leading to risks of unauthorized access and use of inaccurate or out-of-date information. Also, some users intentionally work around planned controls when using the authorized systems; for example, the practice of sharing CHCS sessions.
- Internet Access: Many MTF staff members do not understand the security risks associated with downloading information from the Internet and do not appreciate the impact of such activity on bandwidth available to the facility. MTF policy should be reviewed to insure that Internet usage is sufficiently addressed. In addition, MTF staff members should receive regular training on the use of the Internet.

At the system level, the organization’s incident reporting procedure varies by system and organizational level and is not well understood. There is no facility-wide procedure for the tracking and follow-up of reported violations and little systematic monitoring to detect unauthorized hardware and software.

ACTIONABLE ITEMS:

Higher Echelons – Support for Security Policy and Procedures:

1. Arrange for a high-level comprehensive review of all DoD and military service policies and procedures to identify gaps and discrepancies with proposed HIPAA rules on data security and medical privacy; as needed, consider the military’s special operating conditions.
2. Provide templates as examples of security policies that multiple MTFs can adapt for their use. These documents should accomplish two tasks: address information security at the operational level, and illuminate the variety of approaches to security that operational components must presently deal with.
3. Mandate standardized approaches to security for the functional systems in operation at the MTF in order to provide an expected mode of operation for all users and administrators.

MTF Management, with Guidance from MTF IT Group Management:

1. Define and approve MTF policies and procedures for information security that comply with the policies and priorities set by higher authority. Assure that policies are sufficiently clear to support proper definition and consistent application of procedure.
2. For those areas where the practices are ambiguous or contradictory, identify and work with higher authority to clarify and standardize.
3. Assure that procedures identify responsibility and that the responsible position carries appropriate authority.
4. Define and implement formal procedure for assuring policy compliance. Include instructions for reporting and processing security violations, applying appropriate action, and tracking/following up on reported violations.

5. Define and implement procedures for requesting exceptions to approved policy and procedure. Include instructions for filing the request, for documenting reasons and terms related to any permission given, and for performing follow-up checks to assure that the permitted practice does not cause exposure of sensitive information. Include in the review process for exceptions the examination of the reason for the exception. Exceptions may indicate that some systems are operating out of the set and agreed bounds.
6. Establish "sunset" provisions for each exception granted including the duration of the exception and the conditions that cause revocation of the exception granted. The end goal is to understand the rationale for exceptions and, if necessary, grant temporary exceptions until root causes are addressed.
7. Establish procedure to periodically review the effectiveness of existing policies and procedures. The intent of the periodic review should be to identify and address systemic problems. Include in this a review of risks introduced since the last review (e.g., changes to departments'/staff members' responsibilities, physical changes to the facilities, evolutionary changes to capabilities of internal/external hardware and software, etc.).

STAFFING SUPPORT IMPACT ON SECURITY POLICY AND PROCEDURES

Staff resources dedicated to formulating, implementing and monitoring security policy and practices need to be adequate and they need to provide defined guidelines of responsibility and authority. They should receive sufficient technical and general training to competently carry out their responsibilities. Staff resources with operational responsibility affect the organization's ability to follow stated security policy. If the staff is not aware of appropriate information security procedures, or if staff is under-resourced and over-tasked, then the priority for protecting sensitive information will slip. The DHIAP Team based their conclusions on interviews with MTF staff and observations made while at the MTF site.

MANAGEMENT OBJECTIVE:

Staff resources are assigned responsibility for information security and given authority to implement security policy and procedures. The actions of operational staff users are in compliance with stated information security policy and procedures.

OBSERVATIONS:

Staffing support affects two areas: operational support to the functional elements, and security staff support to the entire organization.

Operational Support Functions:

The application systems that support the MTF primary functional requirements are often mandated by organizations outside of the MTF, such as MEDCOM, TIMPO, and USAMISSA. Department Units within the MTF often inherit the operations and

maintenance of mandated systems supporting their departments. The responsibility for information security is usually assumed along with the operational responsibility.

The DHIAP Team found that the staff members responsible for operating functional systems were not well grounded in accepted information security practices. The strategy observed was assignment of experienced functional users to manage these mandated systems with reliance on centralized remote administration augmented with books of detailed routine instructions for local operations. The weakness with the implementation of this strategy is that system managers, although experienced in the functional area, have limited systems administration background and therefore are not well equipped to determine policy or set procedures. This is compounded by the lack of standardized policy guidance and the limited resources directed toward information security.

The myriad of systems also impacts the IT resources with unique, changing, or increased demands on staff resources. For example, technical system administrators have to adapt to manage a variety of system configurations; application and technical troubleshooters are required to respond to multiple systems; and application users must respond to a number of differing system operations policies. Limited training is provided to enable the various MTF staff to adequately meet these responsibilities, and little or no consideration is given the MTF for handling the extra costs (user and technical staff resources, implementation process, training, materials) associated with implementing the systems.

Security Staff Functions:

The DHIAP Team viewed the security staff as consisting of individuals assigned primary staff responsibility for security and additional personnel from diverse operational areas who were assigned particular security-related responsibilities. Technical assistance support staff included security in their oversight and assistance duties. Functional staff members were assigned as additional duties the task of liaison with the IT staff in matters regarding system operations and security.

The DHIAP Team observed confusion about the roles, work responsibilities, reporting responsibilities, and authority of MTF departmental staff who are assigned to support the security function. Where the function of Security Manager has been established, the role has been given responsibility with limited authority and control, making it difficult or impossible for security staff to meet the security requirements. The security manager has limited training and experience in security practices and technology. Staff members augmenting the security department were found to be inexperienced in the information security area and have only limited training. Generally, training available is the same as given to users and training in technology-specific areas (e.g., "Introduction to NT") is limited.

Security staff is often assigned multiple duties and responsibilities, stretching resources and creating priority conflicts. Available staff time is not sufficient to competently perform the work (e.g., password management) that assures compliance with security policy.

In general, MTFs lack sufficient dedicated resources to implement stated security policies and to effectively monitor compliance. The dedicated resources need to be augmented by knowledgeable and motivated staff.

ACTIONABLE ITEMS:

Higher Echelons:

1. Examine the command-wide need for information security resources and budget appropriately.

MTF Management:

1. Assign one individual to be responsible for overall security of information systems and patient data at the MTF. That individual should have sufficient expertise to advise the commander on matters that will adversely impact the MTF security. Along with the responsibility for system security, the responsible individual should have authority to develop and mandate necessary policy and procedures to address the significant areas of risk facing the MTF.
2. Evaluate staff responsibilities for potential realignment. System managers should be responsible for meeting mission requirements of the systems they manage. They should have ready access to guidance on matters dealing with sound security practices from the IT staff experts. The operation of the systems, even when under direct control of the functional organizations, should receive close supervision and monitoring from the IT staff.
3. Define the department structure, job responsibilities, staffing, and staff credentials/experience necessary to carry out the MTF security responsibilities as defined in MTF security policy/procedure and the accreditation package. Where the staffing resources or organization structure are found to be inadequate to carry out all responsibilities, negotiate with Command, MTF and departmental leadership to assure adequate coverage of subjects that represent the highest risk to the MTF and arrange for use of staff from other departments as appropriate. Identify the resulting organization as a budgetary issue if necessary.
4. Assure that all security decisions are made (and policies/procedures developed) using a cross-functional team with representatives from clinical, administrative and IT areas so that rules are made with full consideration of the advantages, disadvantages and consequences to each area.
5. Assure that early planning for new systems to be implemented at the MTF includes a review of the staff and skills required for supporting and using the systems. Identify how the MTF will meet all skill/staff requirements, and assure formal arrangements are made to provide staff to: install/test the system and train users, provide ongoing technical system support, provide ongoing user assistance and troubleshooting, perform timely password maintenance, etc.
6. Make the secure operation of the various systems a matter of Command interest, as a failure in connected systems may impact the entire system.

MTF Security Management:

1. Develop and enforce standard policy dealing with the details of operating interdependent systems in a secure manner.
2. Develop and deliver training for departmental security staff on MTF security policies and procedures. Provide extensive orientation on the MTF facility and operational policies and procedures and on information security shortcomings and problems experienced in the past, and provide full information about regulations and outside authorities (e.g., accreditation package) to which the MTF is responsible.
3. Based on results of a skill assessment, develop the expertise of the dedicated security staff in areas integral to their job responsibilities (technical security of systems, development of security policy and practices, MTF departmental processing, technical subjects such as networked communications, etc.).
4. Negotiate with departments whose staff performs security-related responsibilities (e.g., to serve as Terminal Area Security Officers) to: agree on the work to be done, allocate adequate staff time for the work, and define the reporting responsibilities to the home department vs. the IT Group.
5. Periodically review the security organization's structure and responsibilities in relation to changes in the MTF organization. As appropriate, work with MTF management to alter security policy and/or security staff responsibilities and techniques to correspond more closely with the priorities and flow of work of the MTF.
6. Provide initial and refresher training to MTF staff on the facility's security policy and procedures. Training should be refreshed when the procedures change and whenever personnel are assigned new duties. Incorporate security training into the MTF annual training program.

EXTERNAL ACCESS TO MTF SYSTEMS AND APPLICATIONS

Access to the MTF systems and applications should be readily available to support operational requirements. It should also be accomplished in such a manner that sensitive information such as patient data is not exposed during transit or at the remote location. System integrity, i.e., the ability to control access to the internal system and to monitor user actions, should not be compromised by external access. The DHIAP Team based their observations on an examination of three primary objectives of remote access: access to patient information; access to electronic mail and other office automation type support functions; and administration and maintenance of systems and applications from centralized locations.

MANAGEMENT OBJECTIVE:

Remote access to the internal systems will not compromise the integrity, security, or availability of healthcare information, the systems, or the network.

OBSERVATIONS:

The DHIAP Team observed that medical information systems at the MTF have evolved into an interdependent system of standalone systems. Systems with varying degrees of certification (DOD Standard 5200.28) interconnect with each other, with other DOD and MEDCOM elements through the DISA networks, and to the rest of the world via the Internet. This results in a powerful capability that carries with it some significant risks: a physician can connect to the Internet via the local commercial Internet provider, telnet to a CHCS system, and review patient data at home. However, passing this sensitive but unclassified data across commercial circuits with no security violates both Army security guidance and the Privacy Act.

The paths provided for the physician's use in the above example also provide a path for potential compromise of security or integrity. Information passed over the interconnected systems, and therefore at risk, includes user IDs and the associated passwords. A determined intruder could pose as an authorized user and exploit a captured user ID and password to access patient medical records, provider data, and entire medical databases. Further, once the system has been penetrated, an accomplished hacker could use the compromised system as a pathway to other military medical systems both those located within the MTF and those connected to the MTF via the trusted medical network. At the time of the DHIAP visit, no measures for securing the Internet traffic or the patient traffic were in effect.

It should be noted that the MTFs examined are in the same position as many other commercial and government organizations. The growth of capabilities supported by emerging technology has outstripped the maturation of guidance and direction on implementing secure Internet and networked technology. While technology exists to provide security for sensitive information while in transit, implementation requires changes to user and system interfaces. Those changes have been deferred pending revision of the primary military healthcare systems.

A separate issue from using unsecured communication for operational support is the issue of remote access for administration and maintenance. In several cases, System and Network Administrators who have privileged access are outside MTF Command authority, with responsibility for systems' operations broadly distributed across the MEDCOM. A sound economic rationale is that it is easier and more economical to train a small cadre of technical experts at a central location than it is to train administrators at every system site; the issue here is one of safe practices. To gain access to the systems being maintained requires passing root or super user identification and passwords across the connecting network. A determined intruder could capture those user IDs and associated passwords using them to compromise the entire interconnected system. Using the public network with security control limited to that provided by the MedNet frame relay could expose the proverbial keys to the castle.

Remote administration also introduces the questions of responsibility and authority for ensuring secure operations of the mandated systems, and of the controls that should be applied for those systems to connect to a trusted network. The MTF will be held responsible for the safe operation of the network, the systems attached to that network, and the sensitive information accessible on that network although they have little or no control over remotely located unknown agents. Where a third party performs software

installation, there is no standard procedure for giving and removing access to the installer or for ensuring compliance with MTF policies and procedures. Since the externally administered systems are treated in most instances, with the same trust as others on the network (i.e., not isolated from the “trusted” systems), there is some concern that outside administrators could gain access to trusted systems. It was reported that locally introduced changes to increase security were undone by the remote agent. There is also some concern that outside administrators could gain access to information beyond the boundaries of the maintained systems.

The remote system administrators perform some work in a manner that is unsafe. Insecure methods in use for remote system administration include shared passwords and absence of techniques for encrypted authentication and verification. In a number of cases, MTF personnel have only limited knowledge of some of the systems they support. They lack the training and skills necessary to understand, monitor, and audit activity on such systems, and do not always have the time to carry out their responsibilities.

It appears to be common knowledge at the MTF that allowances are made to relax security in order to promote operational efficiency and effectiveness. While the operational need makes sense, little work has been done on exploring alternative approaches that would provide the required operational capability without endangering the system and information security.

ACTIONABLE ITEMS:

Higher Echelons – Support for Security Policy and Procedures:

1. Establish Command guidance for providing and managing remote access. That guidance should include programmatic guidance directed at ensuring strong identification and authentication of remote users and protection of sensitive communication from interception.
2. Establish command-wide security requirements for user access, user identification and password, auditing, information security, remote administration, and secure use of the network-enabled tools such as e-mail and Internet.
3. Include terms and conditions in external agents contracts to ensure that protected health information available to external agents remains confidential and would not be used or disclosed in ways not permitted to the MTF itself.

MTF Management:

1. Establish local policy and procedures for Internet access via MTF system resources.
2. Establish local policy and procedures for remote access via Internet or dial-in to MTF systems.

IT Group Management:

1. Secure critical network resources (e.g., DNS, routers, and bridges) from external access.

2. Isolate remotely administered systems from each other and from the MTF network. Ensure that existing trust relations⁴ with remotely administered systems are well understood and approved.
3. Implement use of strong identification and authentication techniques for remote access to all systems.
4. Implement a procedure for working with external individuals who must remotely administer MTF systems. Include requirements to: acquire certification of “trusted status” (need to know) for each request for access to the system; assure outsiders are aware of and comply with MTF policies and procedures; and audit remote access transactions for compliance with MTF procedures.

SYSTEMS ADMINISTRATION

In addition to the efficient organization and operation of their systems, Systems Administrators are responsible for the permissions and services accorded to internal and external users. Their system configuration choices result in allowing or denying specific services to authorized users and to the outside world. These are critical decisions, and they may allow unintentional weakening of system boundaries both internally between systems as well as at the boundaries to the potentially malicious outside world. Because of the diversity and criticality of the systems administration functions, the area dealing with those functions are further broken into sections of observations and recommendations dealing with the critical components of the administrators' responsibilities.

Systems Administration - Configuration

Administration of system configurations addresses the services, software, and hardware used by user, server and application systems. The DHIAP Team based their observations primarily on the technology review and interviews with the technical staff.

MANAGEMENT OBJECTIVE:

All systems (NT servers, NT clients, Windows 95, Unix, and VMS) are configured with minimal services essential to supporting the mission requirements.

OBSERVATIONS:

As delivered to and used by the MTF, configurations of many systems will not meet generally accepted security practices or DoD, Army, and MEDCOM regulations. Subjects where variances were found include: discretionary access control, auditing, auto-logout, world writeable user and system files, use of most restrictive permissions for

⁴ A trust relation is a willful granting of trust from one party to another. In this case the trust relationship deals with the question of how much the MTF, who is entrusted with the security of the MTF systems, is willing to trust remote administrators, the systems they administer, or systems that may connect to the administrators' systems. Note that refusing to delegate trust does not mean that the agent is not trusted, it may be interpreted as the agent's trust model, i.e., who the agent trusts on their system, is either not acceptable or well understood.

file and directory access, password aging, account management, minimal services and applications, and running unnecessary services. Unnecessary TCP and UDP services were found to be running on several systems, and unnecessary services were found running on client NT workstations. Some services made system configuration or usage information publicly available, while other services could be used to gain unauthorized access to systems. Going beyond the officially procured MTF software, internal procedures currently are weak for evaluating the impact of the installation of non-standard software; there are no tools available to detect and track non-standard software and, because its installation is typically not coordinated with the IT staff, there is currently no way to evaluate the impact on the processing environment.

The preferred and generally accepted practice is to configure systems, whether internal or external, for the minimal set of system services that will support mission requirements. The challenge is to identify this minimal set without hampering operations. Issues that compound the challenge are diversity of systems and standards, remote administrators trying to determine a standard set of services that will not interfere with operations in a diverse number of sites, demands of critical system users for maximum flexibility, and the potential cross-system effects on interdependent systems. The seemingly safest routes for the harried administrator are either to defer the decision of system configurations to default settings or to configure the systems as loosely as possible while keeping potential open holes in mind. These short-range tactics leave the systems open to exploitation. Vulnerabilities in default configurations are well known to malicious hackers and are often specific targets for penetration avenues. Adding to the complexity of deciding system and user configurations are the challenges of staying abreast of new potential exploitation methods as they emerge and of examining new features introduced by vendors to determine whether they introduce new vulnerabilities.

The recognized aid to system administrators is the configuration control board (CCB). The CCB provides a focus point and a decision body to work out acceptable system configurations. Generally they consist of managers and technical expert advisors. The DHIAP Team found that CCB was in place but dealing at this detailed level of system configurations was not within their present scope. They are presently primarily involved in approving standard system hardware and software components.

ACTIONABLE ITEMS:

Higher Echelons –Support for Computer Systems:

1. Establish a Command-level CCB to oversee system configuration guidance and decisions made on behalf of the Command.
2. Include Command CCB representation when making decisions about acquiring command-wide computer systems.
3. Implement procedure for the Command CCB to work in concert with MTF CCBs in defining baseline configuration requirements for MTF systems, servers, and networks.

MTF Management:

1. Establish a CCB to review and approve MTF system decisions and plans. Include MTF management and MTF IT Group technical experts on the CCB to assure their work is based on comprehensive knowledge of the facility and its technical requirements.
2. Implement procedure for the CCB to: define baseline configuration requirements for MTF systems, servers, and networks; evaluate newly delivered systems for compliance with configuration requirements; and review/approve proposed system modifications. Assure that the MTF CCB coordinates its activities with the Command CCB where appropriate (e.g., for defining acceptable baseline configurations).
3. Evaluate the MTF's existing systems for compliance with standard security practice at the MTF and regulations of DoD, Army, and MEDCOM. Where deficiencies are found, take corrective action (e.g., fix the problem, inactivate the system, request exception to regulatory guidance, etc.).
4. Establish procedure to assure that the MTF's IT Group and CCB participate in approving, installing, and testing non-standard software at the MTF.

IT Group Management:

1. Configure systems for the minimal set of system services that will support mission requirements.
2. Acquire software-tracking tools to identify instances of non-standard software being installed and assure that appropriate staff is trained in their use.

Systems Administration - System Services

Systems Services include the basic configuration of services available to the user, standard interfaces for the operating system, and the configuration of certain key elements in the infrastructure such as the Domain Name Server, Simple Message Transfer Protocol, and network management tools. The DHIAP Team reached their conclusions after analyzing the results of the external and internal network scans, the results of scripts run on each machine to capture its configuration, and one-on-one conversations with the technical staff.

MANAGEMENT OBJECTIVE:

Systems are configured such that potential targets of exploitation are understood and vulnerabilities are minimized. System administrators and system managers have policies covering basic systems configurations, follow them, and are trained in the proper methods for configuring and securing systems.

OBSERVATIONS:

Certain MTF system support practices expose the systems to risk. Perhaps most important, it is common practice for a single host to serve multiple purposes as the

network management host, the primary DNS (Domain Name Service) host, and the SMTP (Simple Message Transfer Protocol) host instead of having these services isolated and rigorously secured from compromise. Some specific Observations in this area include the following.

- DNS configuration exposes internal systems: DNS has HINFO (Host Information) and WKS (Well Known Services) entries which provide information that can be used to attack the site. In addition, domain transfer is enabled, allowing the complete DNS table to be downloaded.
- There are a large number of world writeable directories and files on some systems.
- Permission settings are inadequately restrictive for many devices, files, and directories.
- The NT systems are often configured using the default settings rather than in accordance with accepted security practices. For example, some areas are not audited, audit logs are not protected from being automatically overwritten, and guest accounts and default administrator accounts are not renamed.
- Systems are typically delivered with limited or no audit capabilities, and systems personnel are not trained to implement such procedures for the systems they support.

Users who are untrained in systems administration carry responsibility for administration of the application systems. This practice exposes the MTF to risk as these users may be unaware of processes and procedures that would typically be enforced if trained technical staff were performing the responsibility.

ACTIONABLE ITEMS:

Higher Echelons –Support for Computer Systems:

1. Oversee standards applied to system service configurations. Since many of these systems are centrally administered, it is incumbent on some expert oversight authority to ensure that the systems are configured in such a way so to minimize risk exposure.

MTF Management:

1. Assure that IT Group technical staff carries overall responsibility for administration of all MTF systems, including those directly maintained by outside organizations and/or by members of other MTF departments.
2. Assure that a principal from the MTF carries the responsibility to understand, monitor, and audit activity of each MTF system.

IT Group Management:

1. Define and implement department procedure to assure that MTF systems are in compliance with standard security practices and with DoD, Army, and MEDCOM regulations. Working with MTF Security Department, initiate appropriate remedial action and perform follow-up for all systems periodically to ensure continued compliance. Where remedial action is to be delayed or not taken, document and submit to MTF management a summary of the situation, the risks posed, and proposed resolution.

2. Acquire generally accepted automated tools to support the systems administration function (e.g., Windows NT's C2 Manager software) and assure that appropriate staff is trained in their use.

Systems Administration - Network Operation and Services

Network Operation and Services includes the operation of the network infrastructure and the services running on each user and application computer system. It also includes the user connectivity to the hospital via Internet Service Providers (ISPs), modem connection, and military sites. The DHIAP Team reached their conclusions after analyzing the results of the external and internal network scans and the one-on-one conversations with the technical staff.

MANAGEMENT OBJECTIVE:

Policy guidance is available and followed for: Internet usage for web, e-mail and data transfer functions; safe operation and maintenance of systems and software from remote locations; and hospital system access through Internet Service Providers, modem connections, and military sites.

OBSERVATIONS:

Increasing dependency on the Internet for general communications and for performing work remotely introduces certain risks. The MTFs have insufficient policies for use of the Internet, and users are not aware of the proper techniques and tools to use in their work. Non-secure, open communications without encryption or authentication/verification are normal, as there is an erroneous assumption that private network security protects the access and transfer of sensitive information. Examples of sensitive information transferred in the clear include commands for remote system administration, user IDs, and user passwords.

There are multiple unofficial access points to MTF systems and networks, both known and unknown, and limited availability of detailed documentation of the local network architecture makes it difficult to analyze threats. Systems are generally installed with default configurations, enabling unnecessary network services and therefore making these services accessible to the public. Firewalls have not been implemented, and only limited network logging and scanning tools are available for detecting instances of intrusion and analyzing networks and modems. System access requests are not authenticated on a consistent basis. In addition, methods used for external access via modem can put network and sensitive information at risk, as there is no use of such standard protections such as modem detection software, dial-back systems, or encryption of modem communications.

ACTIONABLE ITEMS:

IT Group Management:

1. Define procedures that outline safe techniques for accessing the Internet and performing work via Internet communications.

2. Document existing networks and establish a vulnerability profile for them. Implement fixes for identified problems. Evaluate use of firewalls to protect MTF network communications.
3. Acquire networking tools, modem tools, and intrusion detection tools and assure network administrators are trained in their use.
4. Incorporate modem detection software to identify unauthorized modems providing potential system back doors.
5. Implement strong user identification and authentication systems using such tools as dial back modems.
6. Consider encryption of modem communications to thwart interception of sensitive information on public networks and ISP.
7. Train users on safe use of the internet and automation tools such as e-mail to avoid security breaches from loading and launching applications or opening documents which may contain viruses.

Systems Administration - Passwords and User Accounts

The administration of password and user accounts includes user password selection and the issuing and termination of user accounts on all systems. The DHIAP Team derived these observations from examination of procedures in use to administer accounts and interviews with members of the technical staff.

MANAGEMENT OBJECTIVE:

Password and user account policies are in accordance with accepted security practices and ensure that only legitimate users can gain access to the systems and each user can only access systems and accounts for which he/she is authorized.

OBSERVATIONS:

A system's users are identified and authenticated by a unique identification called a "user ID." Its format typically follows an application standard such as first initial and last name. Used along with the unique identification is a secret password known only to the user and to the system. Creation of the password is normally a personal responsibility of the user, and it should always be a user's personal responsibility to remember the password in order to gain access to the system. Often, if given the opportunity, users will select passwords on the basis of how well they can recall the secret when needed. Satisfying that constraint often means that users pick weak, easy to guess passwords. Often, passwords are written down rather than committed to memory.

The DHIAP Team observed that many users have multiple accounts, each with differing standards for assignment and maintenance of their passwords. This drives users to invent a single password for multiple systems, creating the weakness that discovering one password reveals all passwords. The Team also heard reports of users sharing accounts and passwords to facilitate operational needs.

The MTFs do not have consistent procedures for reinitializing or changing passwords, or for inactivating user accounts at the time of a user's duty reassignment. MTF management of user accounts exposes system and patient information to unauthorized use, as indicated in the following observations:

- Account Creation for New Users: Creating new user access profiles by copying from existing profiles may allow new users to "inherit" inappropriate permissions.
- Account Update with Job Change: MTF processes do not preclude individuals from retaining and accumulating account privileges when changing job functions. A user's access profile may be inappropriate for his or her current job function.
- Account Termination: MTF processes for termination of access are not consistently followed upon employee departure. Individuals who are no longer associated with an MTF may retain access to the MTF's data.

It should be noted that the potential for unauthorized access through "social engineering" was found where, in some cases, system access was granted without preliminary authentication of the request.

In some cases, access privileges were found to be overly permissive. Many accounts had the ability to override volume protection parameters and to change personal privileges. Some systems exhibited inadequate purging of accounts; many of these accounts had high level privileges, and non-existent users or groups owned many of the files and directories. There was no formal record of valid user groups and their members and no method of assuring that purging of a terminated account included removal or archiving of its associated directories and files.

ACTIONABLE ITEMS:

Higher Echelons – Support for Security Policy and Procedures:

1. Develop a command-wide standard for password creation, administration, and use that applies to all systems.
2. Investigate use of technologies that support using a single sign-on to gain access to multiple independent systems.

MTF Management:

1. Define policy for user access to MTF systems that requires single-user, confidential passwords and limiting access to the functions required to perform assigned work. Policy should include the following components:
 - Outline of requirements for related issues such as confidentiality of the password (backed up by user-signed acceptance of the policy);
 - Regular change of passwords based on elapsed time;
 - Change of passwords and privileges based on duty reassignment; and
 - Deletion of access privileges/passwords based on duty reassignment/termination.
2. Establish procedure for documenting management approval of requests for user access to systems.

3. Establish procedure for the MTF to automatically provide IT notification of users' job status changes and for IT to re-evaluate/update user access privileges in a manner appropriate to the status change.

IT Group Management:

1. Establish procedure for management of user passwords and access privileges. Include user-friendly, secure processes for: establishing new user access privileges/password, changing access privileges/passwords, evaluation of requested passwords against criteria defined to prevent use of "simple" character combinations.
2. Obtain appropriate authority to run password-checking tools on all systems to identify flagrant violation of password security practices.
3. Investigate and resolve user access/password issues from the past, including existence of superfluous accounts, files/directories owned by terminated or superfluous accounts, and accounts established for groups of users.

SECURITY TRAINING

The training examined here is limited to security training of end users, technical staff, and security managers and technical training of the IT staff. User knowledge of the operation of the equipment and software, outside of security procedures, is not within the scope of this item. The DHIAP Team reached these conclusions after examining training material and interviewing members of the staff.

MANAGEMENT OBJECTIVE:

Individuals have knowledge of security practices sufficient to support secure operation of the site's systems and applications. Security managers and technical staff have technical foundation in security principles sufficient to apply acceptable security practices to normal operations.

OBSERVATIONS:

Technology is evolving rapidly, and the effect of that rapid evolution is magnified by the complexity of the emerging technology. The challenge is often in determining how to maintain technical proficiency in this rapidly changing technical environment. The technical staff at the sites visited have done a remarkable job in assimilating new technologies in networking, client-server architectures, Internet communications, and a myriad of function-specific systems. The emerging challenge will be to build and maintain proficiency in the area of securing systems.

At the time of the DHIAP evaluation, security training for technical staff, users, and individuals responsible for implementing or assuring compliance with security functions was less than adequate. The technical staff security training and experience did not include training on security practices for specific hardware platforms, and introduction of new systems to an MTF included little or no training on new equipment. Although it is important for IT Group knowledge of information security threats and practices to be refreshed frequently, updates on emerging/current information security threats, actual cases, safe practices, Internet, and the Web are rarely provided by higher level Command.

Users need not only awareness of security issues, but sufficient understanding that they can make a sound decision when faced with alternatives. The users' orientation briefing does not clearly enable users to understand security issues as they relate to their jobs. Many users receive no security training other than the CHCS security module, based on an assumption that the user applies the CHCS training to other systems. However, it was observed that users do not consistently exercise fundamental information security practices. Managers need appropriate level of expertise in this area to evaluate the risks, assess the resources needed to mitigate those risks, and make the decisions on which risks to accept and which to resolve. There is little ongoing training (e.g., orientation briefing, refresher training, Computer Based Training, etc.) to provide updated, specific security guidance to users, and there is no measure of the effectiveness of orientation and annual training.

ACTIONABLE ITEMS:

Higher Echelons – Support for Security Policy and Procedures:

1. Integrate appropriate training in current and emerging requirements for health information privacy and security into career management training in order to ensure that all echelons of command and staff are aware of their responsibilities and authority regarding securing sensitive information.
2. Identify a central source of security awareness training and develop for distribution information suitable for adaptation at the MTF level on safe security procedures, security threats, and actual cases.

Higher Echelons –Support for Computer Systems:

1. Assure that higher echelon staff has received appropriate training in current and emerging requirements for health information privacy as part of their career management field training.
2. As appropriate, require managers of centralized systems to include a security training component as part of new equipment and systems training.

MTF Management:

1. Assure that MTF staff is provided with security training appropriate to their organization role when they join the facility, and that training updates/refresher training is provided on a regular basis. Incorporate information assurance training in to manager development training.
2. Assure that appropriate MTF staff are provided with training in safe techniques for accessing the Internet and performing work via Internet communications.
3. Implement methods for monitoring effectiveness of security training and the user staff's consistency in exercising fundamental information security practices.

MTF Security Management:

1. Assure that MTF orientation training for staff/employees in new positions includes training on security issues that relate to the staff members' new jobs.
2. Develop and provide general security training for all users.

3. Develop and provide security training appropriate for each MTF system, for the users of that system, and for its IT support staff.
4. Assign at least one individual to develop expertise in security with special focus on the site's dominant systems.

IT Group Management:

1. Provide detailed technical training on security practices for specific computer platforms to appropriate IT staff. Regularly provide updated training/refreshers training.
2. Increase staff and user awareness of security issues by providing information regarding current information security threats, actual cases, and safe practices.
3. Provide IT staff training on safe techniques for accessing the Internet and performing work via Internet communications.

DISASTER RECOVERY AND SYSTEM BACKUPS

The area of Disaster Recovery and System Backups is defined as prevention of loss of system access and data and timely restoration of services in case of failure. It includes single user/patient data loss and loss of system and/or data access. The DHIAP Team based their observations on review of disaster recovery policies, visits to computer areas, and one-on-one interviews with the technical staff.

MANAGEMENT OBJECTIVE:

Information assurance policies and procedures are sufficient to assure that full recovery occurs in a manner and timeframe that permits unimpeded operation of the facility.

OBSERVATIONS:

The DHIAP Team noted that disaster planning and recovery was present at each site visited, but also identified areas where the planning could be improved. MTF system backups and disaster recovery plans are inadequate to reliably restore all system operations and data. In some circumstances, even minor problems will result in loss of system operation and data. Plans for Disaster Recovery are incomplete and out of date, not covering all applications and servers and common cause failures could lead to both systems and backups being lost in the same events.

Backups, an essential component for recovering from disaster, are not consistently performed for all operational and server systems. Procedures for retention/rotation of backup media are not sufficient to support restoration of the systems; on many systems the backup media are recycled in less than a month. The "off site" locations where backups are stored are often subject to damage by the same disaster that might strike the production computing environment. In one situation, the Team noted that a single point of failure (a broken tape drive unit) prevented performing system backups.

Protection from disasters occurring within the computers' physical environment is less than adequate. Fire suppression in some critical computer rooms is water-based,

establishing a potential for shock hazard and lose of equipment. Uninterruptible Power Supply (UPS) units are not adequately sized to operate during extended outages, and the older batteries used in UPS units might not be sufficient to allow a controlled power shutdown.

ACTIONABLE ITEMS:

Higher Echelons:

1. Assure that appropriate Disaster Recovery planning is a matter of command interest.

MTF Management:

1. Work with MTF Security Department and IT Group management to prioritize system resources for coverage by the MTF's Disaster Recovery Plan
2. Assure that Disaster Recovery Plans in effect for the facility's computer systems are adequate.

IT Group Management:

1. Review and update the MTF's Disaster Recovery Plan, ensuring it adequately covers the current portfolio of systems and the current physical configuration of the MTF facility. Verify adequacy of retention and storage location for backup media.
2. With Security Department, verify that IT backup/recovery procedure is properly coordinated with user departments' procedures for reestablishing processing capability following a disaster (e.g., paper documents needed to carry operation forward from time of last backup are available for use).
3. Assure all backup/recovery hardware is in place, sufficient to meet current demand, and operating properly.
4. Test backup/recovery procedure for every MTF system and ensure that no single point of failure will result in the inability to backup/recover information and software.
5. Include inspection and evaluation of computer room environment, including: fire suppression, cooling, UPS sizing and UPS battery maintenance in disaster recovery planning.

PHYSICAL SECURITY

Physical security is defined as the protection of computer and network systems, patient records, and individuals from harm, damage, injury and loss. The DHIAP Team reached the conclusions that follow from observing standard practices while on-site at the MTF and through discussions and interviews with MTF staff.

MANAGEMENT OBJECTIVE:

Physical Security policies and procedures are understood, practiced, and verified. Individuals understand and follow the policies and procedures well enough that detection of a violation is immediately noticed, reported to the appropriate authority, and acted upon without delay.

OBSERVATIONS:

In its assessment of physical security, the Team noted that exposures in physical security could be a significant risk for loss of control over sensitive information. Losing an asset such as a workstation is not only a loss of the physical asset but also a potential exposure of the sensitive information stored there. Loss does not have to be something as visible as a workstation; it can also be something as concealable and reusable as magnetic media. Physical security includes not only what may be taken from the area but what can be inserted into the area—for example, a cable sniffing device to eavesdrop on sensitive information inside an assumed closed environment.

Some elements of physical security at the MTF site are inconsistently practiced, jeopardizing information and personal security. In some cases, buildings are open to the public 24 hours a day and in other cases, building security may be easily breached (e.g., through back and side doors that are propped open for convenience). In each case, patient floors and clinics, and the computing equipment located there, are accessible to unauthorized individuals. There are some reports of missing computer equipment. It was reported as difficult to identify or track the missing equipment because property control records are insufficient. Lost with the equipment are any data records stored on the devices.

Another form of physical security is the treatment of the paper and media where confidential information (both patient information and materials marked “for official use only”) is recorded. In many instances confidential information is not destroyed immediately after use; because destruction of patient records is not convenient, the situation worsens as hardcopy patient records accumulate.

ACTIONABLE ITEMS:***Higher Echelons:***

1. Assure that policies and procedures for physical security of patient information exist and are followed at MTFs.

MTF Management:

1. Define a physical security policy, and define/enforce procedures to assure physical security of patient information used at the MTF.
2. Reinforce property control procedures with spot checks of inventory locations (e.g., terminal areas, patient floors, etc.).
3. Evaluate the need for limiting access to each area of the MTF (e.g., records rooms, terminal areas, patient floors, etc.) and install control devices that are appropriate to the situation (e.g., lock and key, combination code locks, badged entry devices, cameras/monitors/staffing, etc.).
4. Identify areas of the MTF where paper copies of sensitive patient data and materials marked “for official use only” are discarded (e.g., physician offices, clinics, registration areas); install devices (e.g., paper shredders) or implement procedure (e.g., deposit in specially colored trash bins that are periodically emptied/contents shredded) to ensure the paper is disposed of properly and in a timely manner.

DHIAP PHASE I COMPOSITE EVALUATION REPORT

5. Train MTF staff on physical security policy and procedures; retrain staff as changes are made. Incorporate physical security training into the annual training refresher program.
6. Perform periodic audits of compliance with physical security procedure and policy, report and act on violations, and define recommendations for updating procedure and policy as the environment changes.

IV. Recommendations and Conclusions

A crucial conclusion that can be drawn from the results of the evaluations is that the security of patient information in the military medical system can be compromised and is at risk. Exploitable vulnerabilities exist, affecting not only the information managed at each MTF but also the integrity of the medical information systems. The sites examined intensely during Phase I are considered to be fairly representative of a typical Regional military MTF and a community hospital MTF. Based on the findings of the DHIAP Information Security Evaluations, it appears that the military MTFs face significant challenges to comply with the existing regulatory guidelines as well as with pending legislative guidance based on provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

There is no single simple solution to addressing the vulnerabilities revealed. Information Assurance involves a myriad of interrelated and interdependent areas. In particular, Policy, Personnel, Operations, and Technology must work together to affect a secured environment (see **Figure 5**). Emphasis on any single area without regard for the other areas will not produce the desired results. The appealingly simple solution of adding

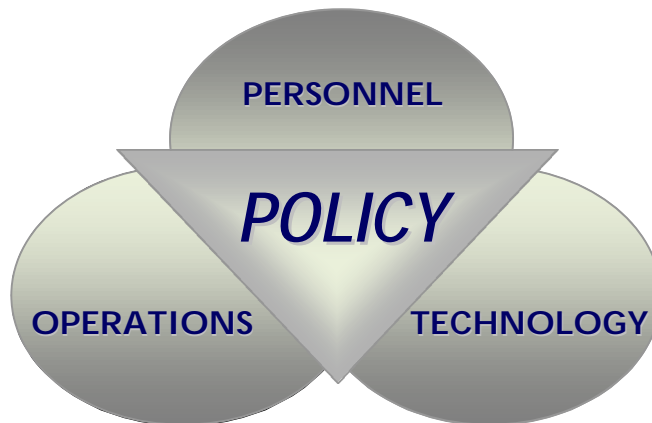


Figure 5 – Key Elements of Information Assurance

more technology cannot provide an instant salvation, nor will the deployment of more detailed policy guidance. Acquiring technology to bolster security, but implementing it incorrectly or poorly, may result in even weaker security. Applying technology without considering the impact on the operations or the personnel involved in maintenance and administration could undermine information security or fail to address the improvement goal. Similarly, policy pronouncement without procedure revision, enforcement, and staff training on implementation will be wasted efforts. There are numerous other examples of well-intended measures that are ineffective because of failure to consider all of the areas that should be addressed. The analysis, conclusions, and recommendations provided in this section are intended to provide the context to guide essential activities and decisions at each level of Command authority that can influence the information assurance posture at the MTF.

DHIAP PHASE I COMPOSITE EVALUATION REPORT

Section III of this report provided observations specific to the vulnerability categories investigated in Phase I and listed remedial actions to be taken by several levels of Command. Section IV, based on the DHIAP Team's analysis of Section III actionable items, groups the recommended activities into management focus areas, broad activities that maintain and control the military operational environment.

Figure 6 is a mapping of recommended management activities to identified vulnerabilities. The Vulnerability Categories shown across the top of the chart were

-----VULNERABILITY CATEGORIES-----										
M A N A G E M E N T F O C U S A R E A S		Org. Climate	Security of Patient Info.	Security Policy & Proc.	Staff Support of Sec. P&P	External Access to Systems & Apps.	System Admin.	Security Training	Disaster Recov.& Backup	Physical Site Security
	Information Protection Oversight	✓	✓	✓	✓		✓			
	Security Policy	✓✓ ✓	✓✓	✓✓ ✓	✓	✓	✓	✓	✓✓ ✓	✓✓ ✓
	Technology Standards	✓	✓	✓		✓✓ ✓	✓✓ ✓	✓	✓	
	Procedures	✓✓ ✓	✓✓	✓✓ ✓	✓	✓✓	✓✓	✓	✓✓	✓✓
	Training	✓	✓	✓	✓	✓	✓✓	✓✓ ✓	✓	✓
	Organizational Responsibility for Security	✓✓	✓		✓✓	✓	✓	✓✓	✓	✓
	Technology	✓				✓✓	✓		✓	

Legend:
✓, ✓✓, and ✓✓✓ indicate the Focus Area's relative impact on the Vulnerability Category

Figure 6 – Recommended Management Emphasis for Resolving Vulnerabilities

discussed in depth in Section III; along the chart's left side are the major Management Focus Areas involved in the DHIAP Team's recommendations. Reading the chart from left to right for a management focus area provides insight into its impact across vulnerability categories. For example, Policy and Procedures each support nearly every area and should therefore receive priority attention. Reading the chart from top to bottom by vulnerability category gives the reader an understanding of the breadth of management activity necessary to adequately address the vulnerability.

The key to protecting military healthcare information will be to establish, enable, and promote a strong security culture, both within and across all participating organizations. The general sequence of activities for doing this is:

- *Establish* the culture –

Identify subjects to be covered by security policy.

Define the security model (i.e., “architecture”⁵) to be adapted and implemented across all MTFs and the related organizations that are part of their business environment (e.g., vendors/maintainers of healthcare systems).

- *Enable the culture* –

Change business methodologies that currently impede or preclude effective protection of sensitive information by revising operational procedures, both within and among the MTFs.

Provide the resources (people, budget, and technical solutions) necessary to define, implement, and monitor daily practice.

Assure that staff training is conducted initially, as procedures are revised, and as individuals’ responsibilities are changed.

- *Promote the culture* –

Ensure compliance with security procedures and mandate meaningful penalties for failure to comply.

Provide continued oversight of the overall information protection architecture to assure it is regularly extended **to address new technologies and operational practices** that are implemented in MTFs and with their business partners.

The remainder of this section provides a brief context of the major operational changes affecting MTFs today, a summary of this report’s recommendations described in terms of the management activities that must occur, and conclusions.

CHANGES AFFECTING MTFs TODAY

The military Medical Treatment Facilities evaluated are involved in several types of change that relate to their ability to meet their information protection responsibilities.

- Migration toward electronic patient record (EPR) systems. Emerging EPR capabilities will support significant improvements in the continuity of care provided to the patient. Some advantages are already apparent: availability of patient information has improved significantly over only a few years ago; coordination of care across providers and facilities has improved; and corporate knowledge of the patient and ease of care-centered collaboration have been enhanced. With these

⁵ Information security architecture will bridge the gap between business process/policy directives and technology-enabled security measures. For example, an organization’s policy for preserving confidentiality of patient data has implications on the way it identifies and authorizes system users, structures its systems access control lists, and encrypts communicated data. Each of these security functions requires that specific action be taken on each hardware platform, in each operating system and network, and within application systems. The architecture should define a minimum acceptable level of technical rigor, as well as a baseline set of audit checks, in platform-neutral terms so the organization can verify whether it is in compliance with policy. In addition, organizations must extend the bounds of their security architecture to cover links they have with various classes of collaborating and cooperating organizations (e.g., third-party system maintainers, outside users, and mobile users). Finally, since it is likely that organizations will continually accelerate efforts to provide information access to any location at any time, they must assure that the established information security architecture is revised in ways that preserve the integrity of control processes while making the needed changes to their middleware and application structures.

advantages comes the issue that healthcare information systems will contain far more sensitive information and will have a larger, more diverse group of users than ever before. It has become more critical and more of a challenge for MTFs to uniquely identify system users, to assure that users have access to only the types of information and the specific patients needed to perform their jobs, and to monitor when, where, and why each user is on the system.

- Introduction and integration of new technology. Realizing benefits from use of a new technology often requires revising current technical processes and procedures. Likewise, effective use of the new capabilities requires that existing operational policies and procedures be reexamined. The goal in each of these efforts is to take maximum advantage of emerging capabilities while protecting against the introduction of new weaknesses that might arise when the new technology operates in the context of the existing work environment.
- Changing operational and regulatory environment. The military will be subject to the information privacy requirements of the new HIPAA legislation in the near future. Also, the business practices followed to deliver and cover costs of care will change dramatically as cost-cutting requirements drive the government to consider and implement new paradigms.

While MTFs are rapidly increasing their ability to leverage information, they must also address their increased risk of exposing sensitive information for unauthorized release and use. The DHIAP Team examined the current state of a number of hospital application systems, focusing on MTF ability to ensure the integrity, availability, and confidentiality of the data and information contained in those systems. The preceding Observations and Actionable Items section of this report contains almost one hundred recommendations for action, some of them redundant since the same or similar mitigation strategies may be appropriate to multiple areas (e.g., training, policy, and procedures). The material that follows clusters those recommendations into actionable recommendation themes, pointing out the unavoidable interdependency between the type of actions that can be taken by individual sites and the *prerequisite* actions that must be taken by higher authorities.

RECOMMENDATIONS FOR MANAGEMENT ACTION

Information Protection Oversight

The DHIAP Team recommends that information assurance be a matter of Command priority and that Command provide oversight of MTF/third party actions to meet individual information protection responsibilities. MTFs need to be successful in protecting sensitive information in an environment where system communications and system selection/implementation require using resources outside direct control of the MTF. They need a powerful information security champion, a central group with authority to oversee joint efforts. Some specific subject areas where higher echelon oversight of programs affecting the MTFs should be applied are listed below.

- Oversee configuration guidance and decisions made on behalf of the Command. A Command CCB should work in concert with MTF CCBs to define baseline

configuration requirements for MTF systems, servers, and networks and guarantee that they include proper consideration for assured operations.

- Identify, recommend staffing for, and provide support to the resources necessary to provide information assurance required at the MTF level.
- Oversee the Army's program acquisition agencies to ensure that mandated information systems will meet established security requirements, include adequate training for both user and systems support, and comply with established security requirements throughout the system life cycle.

At the MTF, a CCB is needed to review and approve system standards and plans from the MTF viewpoint and to promote improvements in local information assurance operations.

Policy

The DHIAP Team found that current security policy and policy guidance is inadequate, primarily because implementation of technology advances has outpaced the development of policy decisions needed to properly manage availability and use of the information contained in healthcare systems. Further, the systems' users have raised their level of expectation regarding functional capabilities to be provided in healthcare applications and are demanding levels of access to data and information that they currently enjoy in other, non-healthcare work contexts. The military's present policy for protecting sensitive information should be revisited in order to align official policy and procedure with today's environment of advanced functional capabilities and increased user expectations.

The MTF policy must be based on doctrinal guidance from echelons above the MTF. This is necessary to assure the thoroughness and consistency of new policy and because the subjects of many critical policies lie beyond the control of an MTF. The DHIAP Team recommends that policy guidance be formulated at the OSD(HA) or MEDCOM level based on DISA and DISC4 guidance and then incorporated into policy guidance for local MTFs. Some important subjects of policy revision or definition are:

- Standards and responsibilities for work performed by organizations that are third parties to the MTF (e.g., system selections, system implementations, communications networks);
- Internet access from a site's facilities, remote access to a site's facilities, and remote administration of a site's facilities;
- Role of patient permissions for use of patient-confidential information, especially in relation to situations unique to the military environment; and
- Site's physical security, with special consideration of its role in protecting computers and data.

Given the current environment of emerging regulations, there must be a specific effort dedicated to incorporating HIPAA requirements into existing policy. In addition, the policy revision effort should acknowledge and accommodate the need for permitting exceptions to approved policies. Often, it is the warranted exceptions that alert policy makers of the need to modify policy to keep pace with changes in the environment. To

encourage policy review on the basis of exception, every exception should be tracked and should include an expiration provision.

For effective promulgation of policy in a highly distributed organization, it is useful to centrally develop standardized formats of local (e.g., MTF) policy, or “*standardized security policy templates*.” The standard templates serve as informative, specific policy guidance that allows each facility to better understand the policy and implement it as envisioned by authors of the policy. By stating the higher echelon’s rules for MTF-level behaviors in template form, the approach allows:

- Centralizing the work of authoring clear policy definitions where policy should be well understood and where the effects of a changing environment can first be measured and dealt with;
- Assuring that authors have considered MTF operational impact and resolved any issues before new policy is published;
- Assuring that policy is understood and carried out consistently across sites;
- Reducing workload significantly at each MTF since the staff there need not spend time on authoring MTF policy and may, instead, focus on tailoring the standard to site-specific situations; and
- Empowering each MTF to require policy/procedural compliance in such difficult organizational relationships as MTF-to-MEDCOM (and other military sources of required systems), MTF-to-third party system vendor, MTF-to-MTF, and MTF-to-Regional IT/operational staffs.

Technology Standards

As presented earlier in this section, technology choices at all levels must be made in alignment with the overall security policy. In the same way that operational policy must be centrally defined and communicated to the MTFs, an information security architecture that reflects policy (i.e., a set of technologies that together enable approved activities and prevent unallowed activities) must be defined. Once in existence, the technology standards are implementable across all facilities and serve as an authoritative reference point when it is necessary to make local decisions about unique technical requirements.

Technologies introduced into MTFs are customarily selected and approved by higher levels of authority. That selection should not only conform to the information architecture but also reflect an appreciation of MTF environments where the technology will be applied. The selection process should include defining standards for the technology’s implementation and use, addressing such topics as: required physical site characteristics, acceptable/unacceptable values of parameters central to the system’s installation and use, materials for training the onsite support staff and users, procedures for maintenance and operational use of the system, and an outline of responsibilities of onsite MTF staff vs. those of external system maintainers and/or users. Besides the obvious advantage of providing MTFs with an approved map of how the new technology is to be implemented and used, the effort of developing and complying with technology standards establishes a joint higher echelon-MTF reference point for dealing with site-specific questions and issues. The IT person at an MTF will have a well-trained higher

authority within the Command (vs. an outside vendor or an equally untrained peer) who is responsible for providing technical guidance, and the Army will have a channel to learn of the issues reported by an individual MTF that should actually be resolved for them all.

It is important to note that the process of developing applicable standards relative to a new or changed technology fosters the decision making process about allowable actions and criteria to be applied. The standardization of key elements related to the technologies used by and among MTFs provides a ready reference for management use in assessing the suitability and potential impact of new systems, as well as for guiding implementation decisions. Since every commander has the obligation to assess the impact of proposed implementations on the organization, these standards provide the proper basis for accepting the proposed implementation, refusing it, or isolating it from other systems so that operations of the MTF are not compromised by the non-standard characteristics of a rogue.

Procedures

Procedures are the implementation guidance for policy; they are the *how* to policy's *what*. Since procedures provide the details necessary to properly implement policy, they should be consistent with policy guidance. It is not possible for all procedures to be defined at the MTF level. For such topics as the external selection, implementation, and administration of MTF hardware and software systems, procedures must be established by the organizations that actually select the systems and mandate their use. Only the system managers, in negotiating with third parties and specifying compliance with procedures in the final contracts, can assure that third parties are held responsible for complying with official military policy and procedure.

At the MTF level, there are both technical and operational procedures to be defined.

- Technical procedures, which are of particular importance as the military sites migrate to using the Internet for communications, would cover how the IT staff implements and operates the site's systems to assure compliance with [higher echelon] requirements. Subject areas include: password administration; definition and maintenance of user access privileges; installation and use of systems (standard "approved" systems as well as the non-standard, private user- and function-specific systems); secure use of network-enabled tools such as e-mail and Internet; remote system access by system administrators and users; management of patient information stored on local media; and auditing of system access by support staff, system administrators, and users.
- Operational procedures would cover how the many types of people working at the site deal with sensitive information in their daily work. Subject areas include: maintaining secrecy of passwords, maintaining confidentiality of sensitive information (on terminals, when printed, when transferred to local computers), etc. Many specific procedural recommendations are enumerated in Section III (Observations and Actionable Items) of this document.

Training

A viable training program in information security is needed to complement and reinforce policy and procedure. Several types of training are needed; each is summarized below.

- **Universal Staff Training:** A command-wide information security and awareness program should be instituted to instruct staff at all levels on approved policy and standards. To assure consistency with policy at the start and going forward, the course should be developed centrally in coordination with the group that develops and maintains the policy guidance for all MTFs. Then, before using the training materials locally, MTF staff should adapt them to reflect site-specific variations to the Command-wide policies, procedures, and standards. For development and delivery of more universal training subjects, Command should encourage the use of Army-provided Computer Based Training (CBT). Because it is developed and updated centrally, it should prove to be the most efficient and effective means of delivering consistent training to the distributed sites.
- **Specific Staff Training:** In addition to the overall operational training, security training appropriate to each person's organizational role should be provided; the course material should be taught to each individual who joins the facility and, as appropriate, each time the individual changes operational roles. Also, an information assurance component should be incorporated into manager development training.
- **System User Technical Training:** Materials for training system users in overall system capabilities and in how to properly perform their work responsibility using the system should be provided with the system, then modified as necessary by each MTF for region-and site-specific variations. Course material should include material on current security threats, actual cases of information exposure, and safe practices. In most cases, fact sheets summarizing security aspects of the technology should supplement the course material.
- **IM Staff Technical Training:** Training in information security should be required for the IT staff and the supporting organizational personnel. IT technical staff with security-related responsibilities should be given detailed training to stay abreast of the rapidly changing threat environment and the countermeasures that are appropriate. In addition, since safe operations is a direct contributor to improved security of operations, introduction of any new hardware and software systems to the MTF must include providing operational training to MTF staff responsible for proper, secured operations.

Organizational Responsibility / Authority for Security

The Team found a misalignment between responsibility for some operations and the corresponding authority to operate the systems securely, resulting in circumstances where it was difficult to determine who would take responsibility to make improvements happen. Areas where responsibilities were not clearly defined involved both systems that were remotely administered and systems where local managers of MTF functional areas held responsibility for performing system administration functions.

To resolve these and other difficulties, each MTF should have a “security” responsibility area with authority to define, oversee, and enforce security compliance throughout the MTF. The leader of this function must be well versed in security policy, procedure, and enforcement techniques, and the security responsibility must be staffed by individuals with experience or training in both security and the relevant functional area(s) of MTF operations. While the leader’s position should be a dedicated resource, the staff positions might well employ staff from IT, functional user areas, or both. The security staff would carry responsibility to implement security into MTF procedures, monitor for compliance, track and make decisions on allowing exceptions, and serve as the first-line problem solvers. To accomplish this, it is essential that functional area users and administrators of the systems (clinical staff, administrative staff, etc.) work as a team.

As a rule, responsibility for the security of MTF computer systems should be shared among IT and the functional system users, with primary oversight responsibility owned by IT. In some areas of the MTF (e.g., laboratory and pharmacy), functional area staff control the system because their extensive knowledge of the work environment qualifies them to assure the system properly meets the department’s operational and regulatory requirements. However, it is often the case that the functional staff are not well grounded (compared to the IT staff) in such essential system-related practices as testing, user training, and operations/backup/recovery procedures. In these cases, it is necessary for IT to support the functional area in its implementation of systems but maintain control over planning and execution of the essential IT components of system implementation and operation. This assignment of responsibility applies equally to all MTF systems, whether they are managed by IT, by internal resources outside the control of IT, or by external resources.

In the technical arena, proper wielding of authority over MTF systems will require that IT staff be well-trained in diverse aspects of operating the systems in a secure manner. Their responsibility for ensuring system safety should include the authority to isolate non-compliant systems from the network so that security weaknesses in one system cannot compromise the entire network of interconnected systems. To assure that IT and user staff continue to be able to operate systems securely, the introduction of any new systems and major system modifications to an MTF should include IT and functional user training in security measures appropriate to the system’s operation.

Technology

Emerging technology has the promise of significantly improving security posture. Implementation of enabling information security technology should be considered and planned for as part of a total security improvement program. Technologies available for application now that are cited in the actionable items of Section III are strong identification and authentication techniques, encryption of communication, single sign-on, and password checking tools. As has been previously stated, an information security architecture that implements an agreed information security policy is the key to making significant improvements in information assurance.

Another factor that raises technology to the level of an important organizational consideration is the complexity and current pace of change in technology. The constant renewal and adoption of new IT products can easily erode an organization’s IT security

framework. Since the technology marketplace features a dizzying array of products that attempt to address a variety of security issues, IT faces a complicated landscape of products and technologies. The workforce must build and maintain their technical knowledge, skills and ability to keep pace with the demands of technology advancements. A plan for continuous training on emerging technology should be part of every administrator's career plans.

The impact on information assurance posture must be a consideration in implementation of any new technologies, not just those technologies particularly focused on information security improvements. For instance, systems should always be configured for the minimal set of system services that will support mission requirements in order to minimize the danger of inadvertent or intentional misuse of system resources. Technological tools can assist in evaluation and improvement efforts at the MTF level by enabling monitoring functions such as identification of non-standard software, intrusion detection, modem detection, and network monitoring. Of course system administrators must be trained in tools use and the use must be incorporated into operational procedures.

Finally, the daily administration of the complex network of systems that have evolved in the MTF must include emphasis on information assurance. User's access and passwords from superfluous accounts, files and directories ownership, and group accounts should all be examined routinely and resolved to assure that responsibility and authority for user access is clear and unambiguous. Backup recovery hardware and procedures must be sufficiently sized to meet current demand and routinely checked for proper operation. In prioritizing efforts, critical network and system resources such as domain name servers, routers, and bridges, should be secured from any external access.

CONCLUSIONS

The DHIAP work reported here was designed to be a vulnerability identification effort followed by an insertion and demonstration of technology to address some of the higher priority vulnerabilities (e.g., the RADIUS prototype effort that is also part of DHIAP Phase I). The DHIAP Team is currently in the process of accomplishing the technology insertion but has recognized that technology insertion is necessary but not sufficient to resolve the security issues. Many solutions require that all four of the synergistic and mutually supportive areas depicted in **Figure 5** be addressed together. The technology is easy. Driving behavior is the difficult part because it requires coordinated effort among many different actors and agents. We have observed that technology insertion, such as the DHIAP RADIUS demonstration, can serve as a focal point for driving behavioral change because it brings staff attention and closer scrutiny to issues surrounding information assurance and provoking change for the better.

The information security evaluation work resulted in identification of a wide range of vulnerabilities that could impact information assurance at the MTF as well as specific recommendations to address each area. In some cases, the activities required to resolve the vulnerability lie completely within the responsibility, authority, and capability of the MTF. Here, actions that can be effective should be applied as soon as practical. In addition, remedies that are effective at mitigating vulnerabilities at the test sites should be evaluated for application at other MTFs with similar situations. For other vulnerabilities,

however, the actions required to accomplish change are beyond the authority of the individual MTF and will require decisions and actions by higher echelons.

A presently missing element is a comprehensive security strategy for health information assurance that addresses each operating level within the military medical domain, from the MTF to the MEDCOM. This report may serve as a catalyst for developing that security strategy. The strategy should be built on:

- Clear Security Vision: Recognition of the risks that organizations composing the enterprise can tolerate;
- Commitment: Senior management buy-in and resources to execute the strategy;
- Training: Implementing security as part of the normal operations at all levels; and
- Accountability: Clear delineation of who carries responsibility for doing what and a mechanism to measure progress.

There is no need to defer actions to evaluate, prioritize, and assign responsibility for addressing the recommendations within this report until after a sound security strategy has been developed. Rather, this should be an opportunity to pursue parallel and supporting efforts to develop the strategy as an ongoing activity while taking appropriate action to address the recommendations.

The importance of a security strategy will increase as regulatory and legislative guidance continue to place increasing emphasis on security and privacy. In addition, the pending regulatory guidance driven by the HIPAA legislation will cause increased attention to information assurance on the part of accrediting bodies. Implementing the recommendations included in this report will establish a firm foundation for future efforts to comply with the forthcoming laws and regulations. Planning for implementing appropriate measures in accordance with the recommendations found in this document will require coordinated actions within the MTF, as well as support and guidance from the echelons above the individual MTFs. This document provides a mapping of activities to major areas requiring attention and insight into crosscutting corrective activities. The information should be sufficient to establish the basis for setting priorities and describing responsibilities and necessary action steps.

V. APPENDICES

DHIAP PHASE I METHODOLOGY

APPENDIX
A

DHIAP Phase I Methodology

INTRODUCTION

The methodology used in the Defense Healthcare Information Assurance Program (DHIAP) Information Security Evaluation (ISE) was adapted from evaluation processes

initially developed by the Software Engineering Institute (SEI). This Appendix describes the activities performed in each step of the DHIAP's implementation of the methodology, depicted in **Figure A.1**. In the Figure, the rectangular shapes represent the DHIAP Team's activities to plan, initiate, and conclude Phase I activities. Oval shapes in the center portion of the diagram identify the major steps

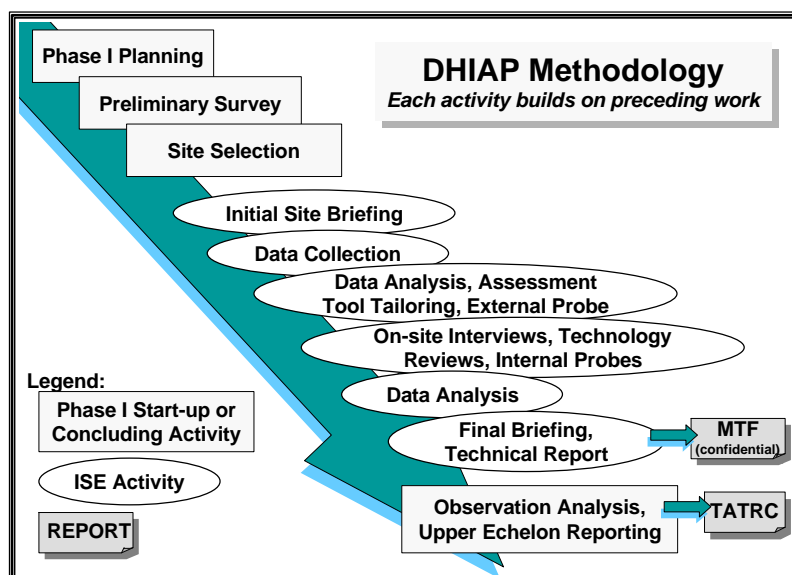


Figure A.1 - DHIAP Methodology

of the ISEs that were conducted at the military Medical Treatment Facilities (MTFs). As implied by the sequence of shapes along the arrow from upper left to lower right in the Figure, each activity of the DHIAP Methodology builds on the results of preceding work.

DHIAP PREPARATION FOR CONDUCTING ISEs

Phase I Planning. Planning for DHIAP Phase I required identifying military Medical Treatment Facilities that would participate in identifying characteristic system vulnerabilities and demonstrating new DHIAP-developed tools and techniques to reduce or eliminate the exposure. DHIAP was designed to begin by establishing a baseline of the current state of information assurance in a representative set of military MTFs. That

baseline would provide the roadmap for the next step in DHIAP Phase I, addressing problems found with current MTF information systems to demonstrate improvements in policy, practices, and technology employed at each participating MTF. Since information derived from the initial set of sites is assumed to represent the problems and issues associated with military MTFs in general, the selection of an initial set of participating sites that would be representative of the larger population of MTFs was key to the success of the effort.

The site identification effort was scheduled for completion within sixty days of initiation; concurrent with identification activities, the DHIAP Team received training on the ISE process. Site selection included gaining site commitment to (1) the ISE process and (2) follow-on participation in the demonstration. The DHIAP ISEs were projected to require a minimum of eight weeks elapsed time per site. When possible, concurrent activities were scheduled so that multiple sites could be evaluated in the time allocated. Schedules called for all ISEs to be completed within five months of site selection.

Preliminary Survey Development. Military and civilian DHIAP Team members worked together to develop a Preliminary Survey questionnaire for use in profiling the security-related aspects of an MTF's technical and operational environment. Supporting materials provided a brief background about the study, instructions for completing the survey, and named TATRC's point of contact for the study; the Survey itself consisted of several pages of questions to be answered by site personnel.

The Preliminary Survey, included as **Attachment 1 to Appendix A**, was designed to gather high-level information about the major areas to be covered in an ISE. Types of information covered in the questionnaire include: a profile of the organization's staffing and prior experience; an overview of the facility's systems and networks; information about the facility's policy and actual practice related to security of patient and other sensitive information; and an overview of types of external access that occur in the system's information processing environment.

Site Selection. As the government's sponsoring organization for DHIAP ISEs, TATRC nominated specific candidate sites for the study. TATRC sent each nominated MTF a letter explaining the ISE process, its advantages, and the commitment requirements for sites participating in the ISE. Enclosed with the letter was the Preliminary Survey, instructions for completing it, and deadlines.

Based on information in the completed surveys and the sites' willingness to commit the appropriate staff resources, TATRC selected candidate MTFs for Phase I participation. The TATRC sponsor and the DHIAP Principal Investigator visited each of the selected sites to brief the commander and staff on the objectives and requirements for the ISE and its follow-on activities. (A copy of the presentation used at the Site Overview Briefing is included as **Attachment 2 to Appendix A**.) They verified the site's commitment to DHIAP and developed the initial plans and schedule for conducting its ISE. During the meeting, MTF senior staff named the site staff member who would serve as the site's designated ISE "On-site Coordinator," then the group discussed and resolved operational issues and scheduled the critical dates for the ISE.

DHIAP PHASE I METHODOLOGY

ISE ACTIVITIES: (1) Preparation for On-Site Investigation

Initial Site Briefing. ISE activities began with a meeting at the MTF between DHIAP Team leaders and the site's senior staff to define specific plans for conducting the study, set timeframes, and designate the types of MTF staff who would participate. Following the briefing, MTF personnel arranged for staff availability for providing specific additional technical and organizational information to the DHIAP Team. To improve DHIAP Team members' understanding of unique technical and clinical characteristics of the site, the group reviewed portions of the MTF's Preliminary Survey responses.

Data Collection. At the initial site briefing, the DHIAP Team provided a detailed Site Survey to the MTF's Chief Information Officer (CIO). The CIO, through the On-site Coordinator, arranged for appropriate MTF personnel to provide the requested information and return the completed survey. The Site Survey's questions had been organized to align with MTF staff responsibility areas; the requested information corresponded to subjects covered by the Preliminary Survey, but in greater detail. Questions covered such subjects as: the hardware and operating systems in use at the site; ownership, content, and support arrangements for the MTF's computer systems and network; and hardware, software, and configuration of the MTF's network.

The On-site Coordinator distributed survey sections to appropriate MTF leaders (including administrators of the various computer systems, technical support staff responsible for the office file server, network, and LAN, and administrators for applications such as CHCS, etc.). The staff completed their portions of the Site Survey and returned them to the On-site Coordinator, who reviewed the responses for accuracy and completeness and forwarded them to the DHIAP Team.

External Probe. Using Site Survey responses in combination with additional information gathered through coordinating with the MTF's Information Technology leaders, the ISE team tailored ISE scripts for the External Probe. They obtained specific permission from the site to perform the ISE's Internet-based probe of MTF networks and

systems, then notified site staff and such other interested parties as the Army CERT of the specific date and time that the probe would be performed.

The External Probe used commonly available software tools to identify the types of MTF information that are visible to the public. Major areas addressed by the probe are listed in **Figure A.2**. While the probe's purpose was to document any site-specific information available to people accessing the site from the publicly available network, the probe's scripts and activities were carefully designed to

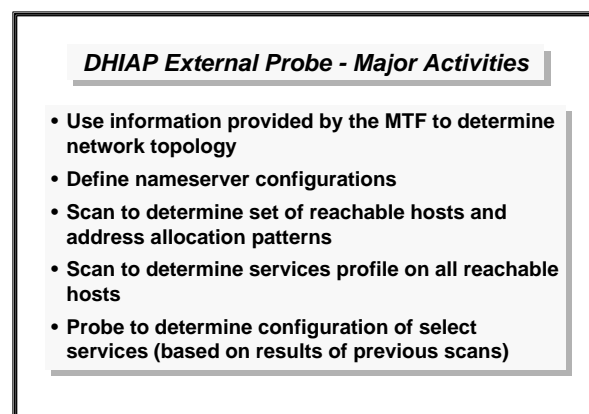


Figure A.2 – External Probe Areas of Coverage

refrain from interrupting or disturbing normal operations.

Data Analysis and Assessment Tool Tailoring. Following completion of the External Probe, the DHIAP Team used its results in combination with information collected via the Site Survey to adapt questions and areas of emphasis for the next ISE activity, the On-Site Investigation. They tailored the methodology's materials for conducting On-site Interviews to fit the MTF's specific technical characteristics and mapped the interview questions to the staff scheduled for each of the site's interview groups. While the Team used the ISE methodology's standard questions "as is" (to assure they covered the same list of relevant areas and used the same phrasing of questions at every ISE site), they adjusted the sequence or emphasis of the questions planned for each interview. The adjustments were designed to assure that (1) subjects were appropriate to the site's technology profile and interview group composition, and (2) the most critical areas of knowledge / concern appropriate for each interview group would be covered in the time allowed. **Figure A.3** provides some insight into how the ISE investigation areas were sequenced to fit the expertise and areas of concern of the different interview groups.

ISE ACTIVITIES: (2) On-site Investigation

On-site Interviews. The DHIAP Team conducting On-site Interviews was composed of an Interviewer, an Issue Recorder, an Official Recorder, a Process Recorder, and Observers. MTF staff represented the diverse roles listed in **Figure A.3**. The interview process paired certain ISE investigators' skills with appropriate MTF staff groupings (e.g., technicians with technicians, clinically grounded DHIAP Team members with MTF clinical staff, etc.).

To protect the interviewees and encourage the free exchange of information, the MTF groupings pulled together staff at similar job levels, usually with related or compatible responsibility areas. Participants were always grouped separately from the staff at other levels in their line of authority (i.e., MTF Information Technology staff were interviewed independent of IT supervisors,

and both were separate from the interview with IT senior management). All interviewees were asked to honor a policy of non-attribution in which statements made by individual members of an interview group or derived from a group's consensus would not be attributed to either the speaker or the group.

The group interviews were scheduled as 1½-hour sessions, all following the same basic process. The Official Recorder took verbatim notes of MTF staff responses to the questions, and, to ensure that all required information was obtained, the interview team often used the responses to the scripted questions as the basis for asking additional, non-scripted questions. "Issues" raised during the interview were recorded in public view on

Group	Typical Group Participants	Interview Areas of Concentration*	
Medical Staff	Physicians (e.g., Family Practice, Internists, Pathologists, Oral Surgeons)	FOR BOTH INTERVIEWS:	
Clinical Support Staff (Application Users)	Nurses Laboratory Technicians Pharmacy Technicians Radiology Technicians	1 - Security Policy 3 - Physical Security 5 - Organizational Issues 7 - Security Violation P&P 9 - Network/System Security	2 - External Connectivity 4 - Assets/Threats 6 - Security Implementation 8 - Services
Technical Area Managers	Network Managers LAN Managers Security Managers	1 - Security Implementation 3 - Security Policy 5 - Vendors/Contractors 7 - Physical Security 9 - External Connectivity	2 - Network/System Security 4 - Security Violation P&P 6 - Assets/Threats 8 - Organizational Issues
Support Staff (Systems, Network, Patient Administration)	Information Systems Specialists Patient Records Staff Medical Records Staff	1 - Security Policy 3 - System/Network Security 5 - External Connectivity 7 - Organizational Issues	2 - Security Implementation 4 - Security Violations 6 - Physical Security 8 - Assets/Threats
System and Network Technical Leaders	LAN Specialist Network Specialist Systems Trainer Application Support Specialists Help Desk Staff	1 - Security Implementation 3 - Security Policy 5 - Vendors/Contractors 7 - Physical Security 9 - External Connectivity	2 - Network/System Security 4 - Security Violation P&P 6 - Assets/Threats 8 - Organizational Issues
Chief, Information Management	Chief Information Officer	1 - Security Policy 3 - Organizational Issues 5 - Vendors/Contractors 7 - Security Implementation 9 - External Connectivity	2 - Assets/Threats 4 - Security Violations 6 - Physical Security 8 - Network/System Security 10 - Services

*NOTE: Although all group interviews were designed to cover the same subject matter, the sequence in which subjects were addressed allowed emphasizing certain subjects (see bold print) based on type of staff represented in the interview group.

Figure A.3- MTF Interview Summary

DHIAP PHASE I METHODOLOGY

whiteboards or flip charts, were reviewed by the group, and were modified as needed to assure accuracy. While it was rare for all of the planned questions to be covered in the time allowed for a single interview, the team did assure that all questions of the standard methodology were answered by the time that all interviews had been completed. Following completion of interviews conducted on the first day of the On-site Visit, the DHIAP Team performed an interim analysis of interview results and adjusted the activities planned for the following day (the Technology Reviews and Internal Probes) accordingly.

Technology Reviews and Interviews. The second day of the On-site Visit emphasized Technology Reviews in which ISE team members used previously obtained information to examine targeted systems. Also, working with the MTF's responsible computer and network system administrators, they examined key security aspects of selected computer systems by examining user permissions and system configurations of the MTF's installed systems and applications. A representative list of the systems examined in this process is included as **Figure A.4**.

- **Technology Interviews** were based on site-specific information derived from responses to the Preliminary and Site Surveys, External Probes of the site, and the observations and issues recorded during On-site Interviews.
- In the **Technology Reviews**, machine- and operating system-specific scripts provided by the DHIAP Team were executed (in cooperation with the MTF system administrators) to collect information about the configuration and characteristics of each targeted system. Each review was tailored to the specific application and to the specific computer's operating system and other technical characteristics.

<i>Infrastructure Technology and Information Systems Examined</i>	
<u>Technology Platforms --</u>	
✓	Network Infrastructure, World Wide Web
✓	Operating System Software (VMS, UNIX, NT, Win 95)
<u>Application Systems --</u>	
✓	Composite Health Care System (CHCS)
✓	Medical Diagnostic Imaging System (MDIS)
✓	Corporate Executive Information System (CEIS)
✓	Third Party Outpatient Collection System (TPOCS)
✓	Ambulatory Data System (ADS)
✓	Theater Army Medical Management Information System (TAMMIS)
✓	Defense Blood Standard System (DBSS)
✓	Mammography Reporting System (MRS)
✓	Defense Medical Logistics Standard System (DMLSS)

Figure A.4 – Technologies Examined

Information collected in the Technology Interviews and Reviews included system type and status, software packages and patches installed, configuration and services of the network, and configuration of the system itself. Results of the Reviews were analyzed by the DHIAP Team, and significant observations became part of the final Technical Report later furnished to the site's Information Management Office.

ISE ACTIVITIES: (3) Wrap-Up and Reporting

Data Analysis. The Team analyzed and correlated all information gathered during the preceding ISE activities and documented their observations regarding the state of information assurance at the MTF at the time of the ISE. Then, applying knowledge of currently accepted practices for protecting information and of methods for securing information from threats known to be prevalent in the immediate future, they provided

site-specific recommendations for MTF actions to improve the site's ability to protect sensitive information.

Final Briefing and Technical Report. Using the Observations and Recommendations compiled in the previous step, the DHIAP Team prepared a presentation to summarize results of the ISE. They conducted a formal briefing for MTF leaders and appropriate staff, then conducted a more detailed briefing for the Information Technology staff and others that had participated in the ISE interviews. Following these briefings, the Team compiled the detailed technical findings that resulted from the External and Internal Probes, formulated recommendations for addressing areas of potential exposure, and provided this site-specific Technical Report to the site's Information Management Office.

DHIAP WRAP-UP OF PHASE I

Observation Analysis and Reporting to Higher Echelons. Following completion of all scheduled site ISEs, the DHIAP Team reviewed observations and recommendations developed to date and used the material to build the DHIAP Phase I Composite Evaluation Report. This "composite" report is the DHIAP Team's recommendation to higher echelons about the management actions needed to accomplish the needed changes in values, attitudes, and practices to secure sensitive information at Medical Treatment Facilities. The recommendations are based on the types of vulnerabilities currently evident in military MTFs and on MTF use of policies and procedures for protecting confidential information.

DHIAP PRELIMINARY SURVEY

The DHIAP Preliminary Survey was designed to gather an initial security/technical profile of sites that had chosen to apply for inclusion in DHIAP's ISE process. The full questionnaire used for Phase I ISEs is included below.


Defense Healthcare Information Assurance Program (DHIAP) SURVEY		
Purpose		
<p>This survey is designed to assist in selecting the DHIAP prototype sites. Sites selected will receive the advice and assistance of systems and security experts and implementation of a demonstration version of a secure health information system. Selection of the DHIAP demonstration site(s) will be based on the health information security profile developed as a result of this survey. DHIAP will demonstrate application of security policy, procedures, technology, and training to healthcare systems based on a requirement analysis by systems and security experts.</p> <p>This is NOT a command inspection. It is designed to be a quick survey of information security practices at your site. This information will be held in strict confidence and will only be used as part of the DHIAP.</p> <p>This questionnaire is designed for short answers that may be inserted in the response column. In some cases, additional explanation or documentation is requested in order to avoid lengthy questions. Request you forward the completed questionnaire with attachments to:</p> <p style="text-align: center;">MRMC-AT, Bldg 1054, Patchel Street Fort Detrick, Md. 21702-5012 Attn: DHIAP Team</p> <p>Electronic versions may be forwarded to security911@tatrc.org. Questions regarding this survey may be directed to Mr. Willie Wright, TATRC, (301) 619-7034 or DSN 343-7034.</p>		
QUESTION	RESPONSE	
0.0	Has your organization performed a security risk assessment and/or accreditation of the medical information systems in the last 6 months. If so, please attach a copy of the findings and recommendations.	
1.0 Organization		
1.1	Provide the name, title and contact information of the organization's Chief Information Officer or Information System Administrator.	
1.1.a	Describe his/her education and experience. Is the position full or part time? If part time what is the percentage of effort?	
1.1.b	Describe his/her responsibilities. If part time state other responsibilities and percentage of effort.	
1.1.c	Describe his/her reporting relationships (Chain of Command).	
1.1.d	How long has this person held the position?	
1.1.e	How long do you expect this person to remain in this position?	
1.2	Provide the name, title and contact information of the organization's designated Systems Security Administrator or Chief Healthcare Information Security Officer.	
1.2.a	Describe his/her education and experience. Is the position full or part time? If part time what is the percentage of effort?	
1.2.b	Describe his/her responsibilities, authority and accountability. If part time state other responsibilities and percentage of effort.	
1.2.c	Describe his/her reporting relationships (Chain of Command).	
1.2.d	How long has this person held the position?	
1.2.e	How long do you expect this person to remain in this position?	
1.3	Provide the name, title and contact information of the individual who has authority to release patient identifiable electronic medical information	
1.3.a	Describe his/her education and experience. Is the position full or part time? If part time what is the percentage of effort?	
1.3.b	Describe his/her responsibilities, authority and accountability. If part time state other responsibilities and percentage of effort.	
1.3.c	Describe his/her reporting relationships (Chain of Command).	

1.3.d	How long has this person held the position?	
1.3.e	How long do you expect this person to remain in this position?	
1.4	Provide an organizational chart of your IS and IS Security organizations.	
1.5	Have your organization done an AR 380-19 security checklist? If so, please attach.	
2.0 Systems		
2.1	List all relevant systems that contain patient identifiable data (CHCS and other clinical systems, CEIS and other administrative, business and finance systems, etc.).	
2.1.a	How many staff users per system?	
2.2	Are there other systems within your site with significant number of users or network impact? If so, please list and describe these systems to include number and type of users and network connectivity.	
2.3	Is your system administration centralized?	
2.4	List major applications used on PCs (e.g. Windows 95, Word, Excel, etc.)	
3.0 Information Systems Security Policy		
3.1	Is there a policy on release of personal identifiable confidential/private health information? If yes, please attach.	
3.2	Does your command have a documented IS security policy? If yes, please provide a copy of the document.	
3.2.a	How is the policy disseminated to your military staff, civilian employees, and contractors.	
3.2.b	How do you document acknowledgement and understanding of the instructions?	
3.3	Does the site have a documented role based access control policy? If yes, please provide a copy of the document.	
3.4	How do you exercise configuration control for software / hardware modifications and upgrades?	
3.5	Is there a process for introducing new equipment (such as hosts, printers, or modems)?	
3.6	Who (by position) is authorized to install hardware devices (modems, printers, disk drives, etc.) on personal workstations?	
3.7	Do users install software and/or hardware on their systems?	
3.8	Do you have a policy regarding the installation of unauthorized, copyrighted software on the system? Describe (or attach policy documents).	
3.8.a	How is the policy enforced?	
3.8.b	How do you detect violations of the policy.	
3.9	Describe your password management policy (for example, one-time passwords, password aging, and password quality) or attach policy.	
3.10	Describe procedures for removal of accounts/access for terminating/transferring users or attached policy.	
4.0 Security Implementation		
4.1	Describe the process of educating staff and employees regarding security policy/plans/practices	
4.2	Describe your security intrusion/attack response plan.	
4.3	What security tools (for example wrappers, COPS, tripwire) are used for system administration?	
4.4	Do employees use virus scanners?	
4.5	What methods are used to audit your systems and your networks?	
4.6	How do you assure that all systems are up-to-date with respect to known security patches, ACERT, etc.?	

DHIAP PRELIMINARY SURVEY

4.7	What authentication mechanisms (e.g., standard passwords, one-time passwords, Smartcards, Biometrics, fortezza) are used and where?	
4.8	Are any inactivity log-off mechanisms used? What type and where?	
5.0 Security Violations		
5.1	Do you have procedures for reporting a suspected security violation? If yes, attach.	
5.2	Could it be determined if there was a break-in to one of your systems? If yes, describe the process or attach documents.	
5.3	Could it be determined if your firewall is functioning correctly? If yes, attach the relevant descriptions of the process or attach documents.	
6.0 Network		
6.1	If you had a network problem, who would you call?	
6.2	How many workstations are supported by the network(s)? How many are smart terminals and how many dumb terminals?	
6.3	Provide a chart or description of networks at your site.	
6.4	What tools are used for network administration?	
6.5	Provide a copy of your disaster recovery plan or COOP.	
6.6	What external network system does your organization connect to?	
6.6.a	How do you make sure you can locate them?	
6.6.b	Can employees configure modems for dial-in?	
6.7	Who (by position) is authorized to install hardware devices (modems, printers, disk drives, etc.) on your networks?	
7.0 External Connectivity		
7.1	Do you have explicit policies regarding the use of the WWW, ftp, telnet, video, and modem connectivity? If so, please attach documents.	
7.2	Do your patients and their caregivers exchange information via email or the internet?	
7.3	Do you allow access to your systems from the outside? If yes, who?	
7.3.a	What technologies are used for such access?	
7.3.b	What services to the outside do you provide with such access?	
7.3.c	If you provide web or ftp services to the internet, what steps do you take to protect the content on your web and/or ftp servers?	
8.0 Vendor Services		
8.1	Are vendors authorized to maintain your networks (i.e., routers, systems, and applications)?	
8.1.a	Is advanced notice required concerning changes?	
8.1.b	Do they have to explain how these changes will affect current systems, etc.?	
8.1.c	Is the maintenance done remotely?	
8.1.d	If so, what kind of access technology is used? (e.g., one-time passwords).	
8.1.e	Do vendors remove all vendor access passwords from your systems when they are no longer under contract?	
8.2	How do you validate vendor changes to your system?	
8.3	Do you provide access to your computing facilities to non-employees?	
8.3.a	Who and what are acceptable justification?	

SITE OVERVIEW BRIEFING SLIDES




Defense Healthcare Information Assurance Program





An information assurance demonstration applied to Military Health Information Systems

- Multi-year, multi-phase program designed to:
 - Further understanding of vulnerabilities inherent in health information systems of the MHS
 - Demonstrate feasible IS protection approaches
 - Research emerging information security technologies


Slide 1



Team Members

	Advanced Technology Institute lead in NIST ATP for Healthcare Information Infrastructure Technology
	Lockheed Martin Energy Systems prime for DOE's Oakridge National Laboratory
	Software Engineering Institute CERT Coordination Center
	Healthcare Open System & Trials Healthcare Information systems consortium


Slide 2



Program Description

- Phase I**
 - Evaluate information system security at designated healthcare sites
 - Design and develop secure system prototype to address identified vulnerabilities
 - Demonstrate secured systems operations
 - Evaluate results and capture lessons learned
- Phase II**
 - Apply methodology to additional sites
 - Apply methodology to additional systems


Slide 3



Information Security Evaluation

- Address policy, procedures, technology, organizational, and programmatic issues
- Requires site cooperation and investment
- Includes technical review and staff interviews
- Generates site-specific vulnerability assessment
 - indicator of information system security across Military Health System


Slide 4



Demonstration System Design

- Select system to secure based on site evaluation
- Challenge is to partition a "segment from the whole" health information system
- Design will include policy and procedure recommendations as well as technology

Slide 5



Demonstrate Systems Operation

- Install and operate secured system to address operational realities
- Train staff, managers, and users
- Objective: leave behind a tangible operational system improvement

Slide 6



Evaluate and Lessons Learned

- Evaluation and lessons learned - an ongoing process
 - Evaluation team and evaluated site to assess effectiveness of evaluation methodology
 - SEI to evaluate ORNL design prior to installation and operation
 - Operation of demonstration evaluated by site, government, and team

Slide 7



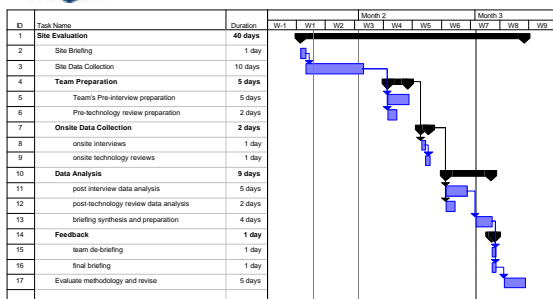
Information Security Evaluation Preview

- Site Preparation Briefing
 - Support, Commitment, Understanding
- Site Data Collection
 - Site coordinator's role - key event
 - Potential probes to understand site configuration
- Data Analysis - Tailor approach to site
- On-site Visit
- Post Visit Data Review and Synthesis
- Results Briefing

Slide 8



Site Evaluation Milestones



Slide 9



Following ISE

- System Selection
- Secure Solutions Design
- Demonstration
- Operation for Validation
- Transition to Site

Slide 10



Follow-on Phases

- Profile vulnerability for military healthcare sites by evaluating additional sites
- Demonstrate scalability of technology by implementing secured system at multiple sites
- Demonstrate applicability of methodology by repeating evaluation / design / demonstrate process on additional systems

Slide 11

APPENDIX

B

Company Profiles and Staff Bios

ATI (Advanced Technology Institute)
<i>ATI has internationally recognized expertise in managing technology programs that deliver the technical depth and unbiased, neutral perspective that can best be provided by a collaborative and cooperative team. ATI has a proven record of delivering technology based solutions to the medical community using teams of collaborating partners, including in-depth efforts in healthcare information protection. ATI provides the overall team leadership, information protection expertise and contract management for the DHIAP effort.</i>
Archie D. Andrews Mr. Andrews is the Director of Information Protection Solutions, an ATI business unit focused on providing services to protect the privacy, confidentiality, and integrity of vital information. He is directly responsible for developing and managing both the technical program and the business development for this business unit. Mr. Andrews brings over 30 years of managerial and technical experience in computer science and software engineering. Immediately prior to joining ATI, Mr. Andrews held the position of Director, Defense Customer Sector and Senior Member of the Technical Staff within the Software Engineering Institute at Carnegie Mellon University. He was responsible for business development and program management of over \$25 million worth of annual work with the Department of Defense and helping to set the technical direction for this Federally Funded Research and Development Center.
Jack A. Stinson, Jr. Dr. Stinson is a Principal Engineer at ATI with over twenty-five years of industrial and academic engineering experience. He is currently the Program Manager for the Rapid-Prototyping of Application Specific Signal Processors (RASSP) Education and Facilitation (E&F) program. His activities with RASSP E&F include managing leading educators and industrial personnel in a distributed team. Dr. Stinson is also the Technical Manager for ATI's Computer Development Lab, which consists of diverse computers and operating systems. He is proficient in several high level computer languages, assembly languages and simulation languages, and has worked extensively with UNIX computer systems and computer networking. He was responsible for establishing the Internet connection at ATI. Prior to joining ATI, Dr. Stinson served as Associate Professor of Electrical Engineering at The Citadel for sixteen years. He taught courses in electronics, communications, digital logic, computer programming, microprocessor architecture and circuits, and was a member of a research team that provided the National Security Agency with background information on the more technical aspects of database systems and local area network response problems.

Lockheed Martin Energy Systems (LMES) Data Systems Research and Development (DSRD) Division

DSRD, as part of LMES' support to the Department of Energy and the Oak Ridge National Laboratory, contributes experience dealing with and evaluating diverse systems that include a security component and training of information security personnel. The ITS staff has extensive knowledge and understanding of national computer security criteria, and the ability to interpret that criteria and apply it to specific hardware/software platforms that are used by or will be used by government agencies. DSRD provides information security professionals, focused on technology design, application and training state-of-the-art technology resources.

Forrest V. Schwengels II

Forrest V. Schwengels, a Senior Data Communications Consultant for Lockheed Martin Energy Systems, Inc., is the Head of the DSRD Networking Laboratory and is the lead technical manager for the DSRD networks. He has over 30 years experience in management, design and operations of complex communications and computing systems. Prior to joining DSRD, he was the Deputy Director and Director of Communications and Computing for the CONUS NORAD Region of the North American Air Defense Command. Mr. Schwengels served for 27 years as an officer in the US Air Force, retiring in 1990. Military positions included Director, Embedded Systems Division, Tactical Air Command and Deputy Director of Plans and Programs, Tactical Communications Division, USAF Communications Command. He is currently providing networking and security expertise to the National Mammography Database/Next Generation Internet Project, the Defense Healthcare Information Assurance Project, the FBI Electronic Fingerprint Image Print Server Project, and several Telemedicine Related Projects.

Stephen L. Packard

Mr. Packard is an information systems professional with over 26 years experience defining, developing, operating and managing systems for the C4I community. Systems have been employed in command posts/centers in Tactical Air Command (Now Air Combat Command), United States Air Forces Europe, Allied Air Forces Central Europe, 3rd Infantry Division, V Corps, United States Central Command, and Marine Force Pacific. Mr. Packard is a retired Air Force Officer now managing Department of Defense projects undertaken by the Department of Energy's National Laboratory and National Prototype Center in Oak Ridge, Tennessee.

Mr. Packard has a BA from the University of Maryland in Foreign Languages, a BS from the United States Air Force Academy in Basic Sciences, an MS from Oklahoma State University in Computing and Information Systems. He has attended the Air Command and Staff College and studied National Security Management at the National Defense University.

Carla H. Decker

Carla H. Decker is a Computing Specialist II – Technical with LMES, currently assigned to DSRD's Communications and Security Department. She has over twelve years of experience as both technical lead and engineering experience in computer science and network architecture and design. She received a B.S. in Computer Data Processing from Florida Institute of Technology and an MCSE from Auburn University in Computer Science with a concentration in network architectures. Ms. Decker is also the laboratory manager for the Department of Energy (DOE) multi-level secure (MLS) local area network that resides at DSRD. Ms. Decker came to LMES from Martin Marietta Corporate where she performed software quality engineering and software engineering duties. She is also a member of the Tennessee Army National Guard and is currently the Regimental Intelligence Officer for the 278th Armored Cavalry Regiment. Prior to joining the National Guard, Ms. Decker spent approximately 6 years in the Army Reserve working assignments for both Fort Huachuca's Tactical Software Division and also served as the Asset Manager for the 1st Military Intelligence Center, an Echelon Above Corps Intelligence Center (EACIC).

COMPANY PROFILES AND STAFF BIOS

Healthcare Open Systems and Trials (HOST)

The HOST consortium, whose members are leading healthcare providers and healthcare technology organizations, has been a leader in rallying the healthcare community to address barriers to the effectiveness, applicability and interoperability of healthcare information systems. HOST provides industry-wide perspective, understanding, and involvement to help ensure that the key healthcare issues are addressed and that the national healthcare community is supportive of the efforts of this program. HOST has also been a key link between the healthcare community and U.S. government agencies. This additional linkage is crucial in attaining consistency with other U.S. government agency efforts in healthcare information protection.

Robert A. Scudder, Jr.

Dr. Scudder is Deputy Director, Healthcare Information Technology, with the Advanced Technology Institute. Additionally, he serves as the Executive Director of HOST. He has over 25 years experience in healthcare as a clinician, health policy analyst, hospital administrator and academician. Before joining ATI, Dr. Scudder served on the faculty of the Medical University of South Carolina, engaging in graduate healthcare management education as well as consultation and research in organizational structures and behavior in healthcare delivery. He led efforts or was a key contributor to the development of innovative new centers in the University, including the Center for Health Care Research, the Center for Rural Health Studies and a doctoral program in healthcare leadership. He remains active with MUSC and currently holds an adjunct faculty appointment in the Department of Family Medicine. Prior career and healthcare experience includes 21 years of commissioned service in the United States Navy Dental Corps. Dr. Scudder performed his undergraduate education at Xavier University and received his Doctorate in Dental Surgery from the Ohio State University. Additionally he holds a Masters Degree in Human Resource Management from Pepperdine University and is a Diplomate of the American College of Healthcare Executives.

Arthur D. Little (ADL)

ADL is one of the world's premier consulting firms, with 2,500 staff members based in 36 offices around the globe. As a widely recognized expert in manufacturing research and consultation, ADL has extensive contract experience pertaining to information handling and technology management for both Government and industry. ADL provides program management support and technical expertise to ATI on a variety of programs.

Thornton White

Mr. White is a Manager at ADL with thirteen years experience working with government and commercial clients in a number of consulting areas. He is currently providing program management support to ATI's Defense Healthcare Information Assurance Program (DHIAP) in the evaluation of vulnerabilities in military healthcare information systems. As Team Coordinator, he is the liaison between the military site and the DHIAP evaluation team, and brings program management experience to the team. Other DHIAP responsibilities include budgeting and scheduling development and analysis for the distributed team members and consolidated team.

Mr. White also provides program management support to ATI in the development of software for security and multimedia transmission and storage of healthcare information systems. Responsibilities include coordination, review, and consolidation of technical and financial information from the distributed team members for presentation to the National Institute of Standards and Technology's Advanced Technology Program.

Mr. White has three years experience as a Test Engineer where he developed test procedures, reviewed requirements, and directed testing of propulsion systems for nuclear submarines. He has an MBA from The Citadel, a B.S. in Chemical Engineering from the University of Florida and a B.S. in Chemistry from Jacksonville University. He is a certified Project Management Profession (PMP) from the Project Management Institute and a registered Engineer-In-Training (EIT) in the state of South Carolina.

Software Engineering Institute (SEI) CERT Coordination Center

SEI provides unique experience and leadership in the area of vulnerability analysis based on its pioneering work in intrusion detection and response including the operation of the CERT Coordination Center (CERT/CC). CERT/CC works with the global community to deal with an increasing variety of threats to the integrity and security of networked computer systems. Its Information Security Risk Evaluation (ISE) program represents the SEI proactive strategy in dealing with information security.

Christopher Alberts

Christopher Alberts is a Member of the Technical Staff in the Networked Systems Survivability Program at the SEI. He is the team leader for security evaluations and is responsible for developing and delivering information security risk management methods, tools, and techniques. His initial focus at the SEI was on developing methods, tools, and techniques for continually managing software development risks. As a result of this work, he co-authored the Continuous Risk Management Guidebook, which shows organizations how to tailor risk management methods for their organizations.

Mr. Alberts is now focusing on applying risk management techniques to networked systems security. He is a qualified team leader for Information Security Evaluation deliveries and is now developing a comprehensive risk management assessment technique that is designed to be self-delivered by organizations. Prior to joining the SEI, Mr. Alberts worked at Carnegie Mellon Research Institute (CMRI) and at AT&T Bell Laboratories.

Kevin J. Houle

Kevin Houle is a member of the CERT Operations team, a part of the CERT Coordination Center (CERT/CC). As a member of the CERT Operations team, he provides technical assistance to Internet sites that have computer security issues, concerns, or have experienced a computer security compromise. He is also involved in developing incident handling training materials and computer security documents. From 1990 to 1998, Mr. Houle served in various roles with Iowa Network Services, Inc. in Des Moines, Iowa. In 1993, he served as the principal technical architect of network and systems used to create and launch netINS, Inc., an Internet service provider subsidiary company. From 1994 to 1998, he served as Manager of Networking Systems for netINS, Inc. During this period he was responsible for developing and scaling network services which eventually became a multi-homed Internet backbone spanning 8 states in the Midwest and supporting 20,000 dialup users, 80 leased line network connections, and 3,000 hosted web sites.

Mr. Houle's technical leadership roles have included direct responsibility for development, implementation, and maintenance of site security policy including engineering a secure infrastructure, responding to security incidents, developing secure services for customers, and providing security consultation to customers.

Suresh L. Konda

Suresh L. Konda, Ph.D. is a Senior Member of Technical Staff at the SEI and a Senior Adjunct Faculty at the Institute for Complex Engineered Systems both located in Carnegie Mellon University. He is currently working in the Network Survivability Systems Program of the SEI and the CERT Coordination Center where he is working in the Security Incident Analysis and Security Management areas focusing on the informational and technical requirements for improving network and system security. Previous to his work in information security, he was involved in developing tools and techniques for software development risk management. He is also working on computer assisted approaches, based on natural language processing, to the analysis of large scale qualitative data. Finally, he is working on the problems of supporting distributed collaboration especially in the context of new product design and development.

Dr. Konda holds a Ph.D. in Urban and Public Affairs and an M.S. in Public Policy and Management, both from Carnegie Mellon University, and a B.E. in Civil Engineering, Madras India. Prior to joining CMU, he was Assistant Professor of Management and Public Policy at the School of Management, Purdue University and Director of the Krannert Computing Center, Purdue University.

COMPANY PROFILES AND STAFF BIOS

Software Engineering Institute (SEI) CERT Coordination Center (cont'd)**James McCurley**

James McCurley is a Member of the Technical Staff with the Software Engineering Measurement & Analysis (SEMA) program at the SEI. He is currently engaged in security projects with the SEI's Networked Systems Survivability Program and continues to collaborate on developing web-based interactive content analyses of Software Capability Maturity Model (SW-CMM) assessment findings data collected by the SEI and published in the Software Engineering Information Repository (SEIR).

Mr. McCurley's previous work at the SEI included a review of the Risk Management Process, development of material for statistical process control in software engineering, and he has taught the SEI's Goal-Driven Measurement course. He received B.A. and M.A. degrees from Carnegie-Mellon University and was named an Andrew W. Mellon Research Fellow by the Carnegie-Mellon Research Institute.

Telemedicine and Advanced Technology Research Center (TATRC)

TATRC is composed of military personnel from all services, along with staff from private industry and academia. Its mission is to provide medical solutions for military requirements to protect and sustain the force. TATRC manages a variety of medical projects in many areas of advanced technologies such as teleradiology, medical informatics, telesurgical robotics and mentoring, and teledentistry. It is responsible for aggressive prototyping and demonstration of new technologies. Through partnerships with other government agencies and industry, TATRC carries out ongoing market surveillance with an eye toward leveraging investigative technologies in health care.

Jeff Collmann

Jeff Collmann obtained his Ph.D. in Social Anthropology from the University of Adelaide, Adelaide, South Australia. Understanding the effect of bureaucracy and other complex forms of organization on everyday life constitutes his main intellectual interest. The results of his research on social change among Australian Aborigines have been published in numerous articles and as a book, *Fringe Dwellers and Welfare: the Aboriginal response to bureaucracy*. Since returning to the United States in 1980, he has worked as an administrator and researcher on issues in high medical technology. While at the University of Tennessee Medical Center in Knoxville, he managed the first clinical Positron Emission Tomography Center and edited *Clinical Positron Emission Tomography* with his colleagues at UTMCK. He completed a Postdoctoral Fellowship in Clinical Medical Ethics, Department of Philosophy, University of Tennessee that produced published research work on the social organization of academic biotechnology laboratories.

Dr. Collmann joined the Department of Radiology, Georgetown University in January 1992. He serves as the team leader for the data security and patient confidentiality section of Project Phoenix, a NLM funded project on telemedicine in hemodialysis at Georgetown University. He is editor of *The CPRI Toolkit: Managing Information Security in Health Care*, a major new resource to aid health care organizations in assuring the security and confidentiality of computerized medical records. He functions as the university co-convenor for Partners in Urban Research and Service-learning, a new initiative funded by Georgetown University to sponsor research and teaching projects between social science faculty and representatives of two inner city neighborhoods in the District of Columbia. He teaches courses in the Center for Australian and New Zealand Studies on the anthropology of Australia and courses in the Department of Sociology in medical sociology and the sociology of science and technology.

APPENDIX C

References

The following materials were used as reference materials by participants of the DHIAP Phase I effort.

- AR 380-19, Information System Security, 27 February 1998
- AR 380-53, Information Systems Security Monitoring, 29 May 1998
- MCUB-AS (25), Memorandum of Instruction: Release of Medical Information and Freedom of Information Act Processing
- MEDDAC Regulation 190-51,
- Military Health Services System (MHS) Automated Information Systems (AIS) Security Policy Manual, Version 1.0, April 1996
- Department of Defense Technical Architecture Framework Information Management, Volume 6: DoD Goal Security Architecture, Version 3.0, 30 April 1996
- Army Medical Department (AMEDD) Information Systems Security Plan (undated)
- Risk Analysis, MEDCOM Network Security Project, Prepared by Science Applications International Corporation, February 5, 1997, for Tripler Regional Medical Center
- Local policy memorandum and regulations on Personnel and Physical Security Program and Security Standards for Automation Data Processing

Note that the pending legislation and regulatory guidance of Health Insurance Portability and Accountability Act of 1996 (HIPAA), expected to be effective in early 2000 and requiring compliance about two years afterwards, will also affect requirements for privacy of individually identifiable health information.

APPENDIX

D

Acronyms and Abbreviations

ACERT	Army CERT
ADL	Arthur D. Little
ADS	Ambulatory Data System
ATI	Advanced Technology Institute
CBT	Computer Based Training
CCB	Configuration Control Board
CEIS	Corporate Executive Information System
CERT	Computer Emergency Response Team
CERT/CC	CERT Coordination Center
CHCS	Composite Health Care System
CIO	Chief Information Officer
CMRI	Carnegie Mellon Research Institute
CONUS	Continental United States
COOP	Contingency Operations Plan
DBSS	Defense Blood Standard System
DHIAP	Defense Healthcare Information Assurance Program
DISA	Defense Information Systems Agency
DISC4	Directorate of Information Systems, Command, Control, Communications, and Computers
DMLSS	Defense Medical Logistics Standard System
DNS	Domain Name Service
DOD	Department of Defense
DOE	Department of Energy
DSRD	Data Systems Research and Development
E & F	Education and Facilitation
EPR	Electronic Patient Record
HINFO	Host Information
HIPAA	Health Insurance Portability and Accountability Act of 1996
HOST	Healthcare Open Systems and Trials
IM	Information Management
ISE	Information Security Evaluation
ISP	Internet Service Provider
IT	Information Technology

LAN	Local Area Network
LMES	Lockheed Martin Energy Systems
MDIS	Medical Diagnostic Imaging System
MEDCOM	Medical Command
MLS	Multi-Level Secure
MRMC	Medical Research and Material Command
MRS	Mammography Reporting System
MTF	Medical Treatment Facility
MUSC	Medical University of South Carolina
OSD(HA)	Office of Secretary of Defense (Health Affairs)
PC	Personal Computer
RASSP	Rapid-Prototyping of Application Specific Signal Processors
SEI	Software Engineering Institute
SMTP	Simple Message Transfer Protocol
TAMMIS	Theater Army Medical Management Information System
TATRC	Telemedicine and Advanced Technology Research Center
TCP	Transmission Control Protocol
TIMPO	Tri-Service Infrastructure Management Program Office
TPOCS	Third Party Outpatient Collection System
UDP	User Datagram Protocol
USAMISSA	United States Army Medical Information Systems Support Agency
UPS	Uninterruptible Power Supply
WKS	Well Known Services

